Hacia una Internet libre de censura II

Perspectivas en América Latina

Agustina Del Campo
Compiladora

Facultad de Derecho
Centro de Estudios en Libertad de Expresión y Acceso a la Información

CELE

UP
Universidad de Palermo

Hacia una Internet libre de censura II

Hacia una Internet libre de censura II

Perspectivas en América Latina

Agustina Del Campo
COMPILADORA

Facultad de Derecho
Centro de Estudios en Libertad de Expresión y Acceso a la Información

CELE

UP Universidad de Palermo

Del Campo, Agustina
Hacia una Internet libre de censura II : Perspectivas en América Latina / Agustina Del Campo ; compilado por Agustina Del Campo . - 1a ed . - Ciudad Autónoma de Buenos Aires : Universidad de Palermo - UP, 2017.
200 p. ; 23 x 15 cm.

Traducción de: Fernanda Guerra ; Jessica Vidal.
ISBN 978-950-9887-20-6

1. Internet. 2. Derechos Humanos. 3. América Latina. I. Del Campo, Agustina , comp. II. Guerra, Fernanda, trad. III. Vidal, Jessica , trad. IV. Título.
CDD 323

Compiladora:
Agustina Del Campo

Traducción:
Fernanda Guerra y Jessica Vidal

Diseño general:
Departamento de Diseño
de la Universidad de Palermo

Corrección:
Carla Ortiz Rocha

Editado por la Universidad
de Palermo, febrero de 2017,
Buenos Aires, Argentina

ISBN: 978-950-9887-20-6

Febrero de 2017

Hecho el depósito que marca la
ley 11.723

Cantidad de ejemplares: 200

Impresión: MPA
Luis Sáenz Peña 647 (1110)
Ciudad Autónoma de Buenos Aires

Impreso en la Argentina / Printed
in Argentina

Universidad de Palermo
Rector
Ing. Ricardo H. Popovsky

Facultad de Derecho

Centro de Estudios en Libertad de Expresión
y Acceso a la Información (CELE)
Directora
Agustina Del Campo

Mario Bravo 1050
(C1175ABW) Ciudad de Buenos Aires
Argentina
Tel.: (54 11) 5199-4500 | Fax: (54 11) 4963-1560
cele@palermo.edu | www.palermo.edu/cele

Este libro fue realizado en el marco de un proyecto auspiciado por **Ford Foundation**.

Índice

Prólogo

Con la diversificación y el crecimiento de internet surgen oportunidades y desafíos que requieren soluciones creativas, que permitan el desarrollo, la inversión, el crecimiento constante, y garanticen los derechos de los usuarios. La regulación es una de las soluciones desde la perspectiva estatal y tiene que estar orientada a solucionar de manera pragmática los problemas que van surgiendo respetando los derechos humanos fundamentales de las personas.

Durante los últimos años América Latina ha visto un crecimiento exponencial en materia de regulación de internet y cierta diversificación de las temáticas que ocupan a nuestros funcionarios públicos, legisladores y quienes día a día están encargados de hacer políticas públicas para el mejor funcionamiento de nuestras sociedades. Uno de los grandes desafíos que enfrentan es que con el continuo desarrollo tecnológico, las problemáticas se van complejizando, y una vez que alcanzamos consensos en torno a ciertas problemáticas, estas cambian, mutan, se agrandan o incluso desaparecen.

Otro factor, no menor, que afecta también la evolución normativa de estos temas es que los desarrollos locales conviven en un contexto mundial. Así por ejemplo, el tratamiento y la regulación que la India propuso en torno al zero rating y los efectos de dicha regulación, permearon la forma de analizar y regular el fenómeno a nivel mundial. A medida que distintos países van "probando" distintas soluciones, a nivel global adquirimos experiencia, por prueba y error, respecto de qué políticas tienen mejores o peores ventajas respecto de las desventajas que acarrean. Uno de los casos más paradigmáticos de esta dinámica en este momento es el fenómeno del "derecho al olvido," una propuesta que nació en Europa y permeó las discusiones en torno al balance de los derechos a la libertad de expresión y a la privacidad de distintos países dentro y fuera de Europa, incluyendo a América Latina.

En vista de los constantes cambios y desarrollos que nos ofrece internet y quienes se dedican a desarrollar las redes, la infraestructura, las aplicaciones y los contenidos, desde el CELE nos proponemos aportar insumos al debate estudiando y evaluando críticamente las experiencias comparadas;

analizando el impacto de ciertas políticas públicas en la vigencia, respeto y garantía de los derechos humanos en internet; y proponiendo, dentro de lo posible, medidas o herramientas útiles para pensar la regulación de manera respetuosa de estos derechos básicos en el contexto latinoamericano. Desde 2010 trabajamos el tema de derechos humanos en internet y en 2012 creamos la Iniciativa por la Libertad de Expresión en Internet (iLEI) prestando particular atención al impacto de la regulación en la libertad de expresión y acceso a la información. También publicamos un primer libro en la materia: *Hacia una Internet Libre de Censura, Propuestas para América Latina*, una compilación de artículos de reconocidos académicos y abogados de Latinoamérica y Estados Unidos que abordaba algunas de las problemáticas más complejas en el desarrollo de la regulación de internet en la región en ese momento. La consigna era identificar las problemáticas y ofrecer distintas perspectivas al respecto tendientes a enriquecer el debate regulatorio y realizar recomendaciones concretas para el desarrollo de políticas públicas respetuosas de los derechos humanos en la región.

En esta nueva publicación, y bajo la misma consigna, se abordan algunos de los temas más significativos que vienen marcando la agenda legislativa y regulatoria en materia de internet en América Latina. Todos ellos presentan aristas y asperezas que generan duros enfrentamientos entre pares académicos, doctrinarios, legisladores, abogados, técnicos, compañías y usuarios.

El primer artículo, escrito por Carolina Aguerre, aborda la gobernanza de internet y las distintas instancias de gobernanza local que se han proyectado en América Latina, evaluando la eficacia de los distintos modelos surgidos. El segundo artículo, de Daniel Álvarez Valenzuela, brinda una introducción al tema de ciberseguridad, destacando la necesidad de enfocar el tema desde la perspectiva de los derechos humanos. El tercer artículo, de Luca Belli, describe la íntima vinculación entre el acceso a internet y el *zero-rating*. Y el cuarto artículo, de Arturo Carrillo, ofrece un análisis del mismo tema a la luz del test de legalidad, necesidad y proporcionalidad que establece el sistema interamericano de protección de los derechos humanos. Los últimos dos artículos abordan la problemática del "derecho al olvido". Daphne Keller ofrece un análisis de la directiva europea en este tema, desde la perspectiva de la protección de la libertad de expresión y su (in)transferibilidad a la regulación latinoamericana; y Nelson Remolina evalúa la interpretación y el desarrollo jurisprudencial del derecho al olvido desde la perspectiva de la protección de datos personales.

El objetivo de esta publicación es precisamente facilitar la comprensión de las distintas complejidades de cada uno de los temas a través del contraste de ideas, a fin de enriquecer el debate público, identificar ventajas y

desventajas, virtudes y defectos, de las distintas teorías y propuestas que se plantean, y colaborar con ello a la creación de políticas públicas necesarias y proporcionadas, respetuosas de los derechos humanos.

Esta publicación se realiza en el marco de un proyecto del CELE con el apoyo de la Fundación Ford. Desde el CELE agradecemos las contribuciones de todos los autores y al equipo que trabajó en la publicación. Esperamos que los aportes sean útiles para pensar la regulación de internet a futuro en estos y otros importantes temas vinculados.

Agustina Del Campo

Capítulo Uno

Redes de gobernanza de internet a nivel nacional. La experiencia de casos recientes en América Latina

Carolina Aguerre[1]

Resumen

Este trabajo examina los mecanismos institucionales de gobernanza de internet en diversos países de América Latina que emergieron en los últimos años, como fue el caso en Argentina, Colombia, Costa Rica, México, Uruguay y Venezuela con el trasfondo del caso brasileño. Desde la literatura en gobernanza de internet, la investigación está orientada a conceptualizar la relevancia de la dimensión nacional. Se considera la formación de estos nuevos espacios como redes de políticas (*policy networks*), en transición hacia redes de gobernanza en el nivel nacional, sobre los cuales se delimita un campo de acción específico. El artículo analiza estos casos nacionales buscando comprender sus variaciones, los aspectos en común y posibles consecuencias de estos arreglos para la definición de las políticas de internet.

[1] Carolina Aguerre es profesora de Nuevas Tecnologías en el Departamento de Ciencias Sociales de la Universidad de San Andrés e investigadora afiliada del Centro de Tecnología y Sociedad (CETYS) de la misma institución. También es investigadora afiliada del Observatorio de Políticas de Internet de la Universidad de Pennsylvania. Es doctora en Ciencias Sociales por la Universidad de Buenos Aires y máster en Communication, Culture and Society de Goldsmiths College, Universidad de Londres. Sus ejes de investigación están centrados en el desarrollo y políticas de la gobernanza de internet, incluyendo el despliegue de nuevas tecnologías y de infraestructuras críticas de internet. Fue directora ejecutiva de LACTLD, la asociación latinoamericana de registros de dominios de internet, miembro del MAG del IGF y del Comité de Programa del LACIGF.

Introducción

Hasta muy recientemente, la gobernanza de internet resultaba un tema marginal en la mayoría de las agendas políticas en América Latina. Los debates se limitaban a algunas agencias gubernamentales especializadas, un grupo de académicos y unas pocas ONG. Pero a mediados de 2013, las revelaciones de Snowden sobre la vigilancia masiva en internet transformaron radicalmente las discusiones en torno al tema. En la actualidad, estos asuntos se discuten en los medios de comunicación masivos así como en algunos eventos, como en la reunión de Netmundial en San Pablo, en abril de 2014, que logró concitar la atención de secretarios y ministros de Estados.

Es importante detenerse sobre esta reunión de Netmundial y el papel de Brasil, ya que alimenta directamente el objetivo de este trabajo vinculado al desarrollo de mecanismos nacionales de gobernanza de internet. Esta conferencia no hubiera podido realizarse en ese país si no hubiera existido el respaldo y la trayectoria del Comité Gestor de Internet (CGI) y su modelo multiactor de gobernanza de internet. Durante 2013, la posición de Brasil como actor global en la gobernanza de internet se volvió un hecho indiscutible. Ningún Estado logró a la vez expresar de forma tan contundente su malestar ante el esquema de vigilancia ubicuo desarrollado por la NSA[2] de los Estados Unidos, ni coordinar una acción conjunta de alto nivel para abril de 2014 con diversos actores involucrados en la gobernanza actual de internet. El propósito era abordar la problemática de una internet abierta y segura que, a la vez, garantice la privacidad y la libertad de expresión. Este papel de Brasil –entendido como el Gobierno, pero también como los diversos actores de la sociedad civil, la universidad y el sector empresarial de ese país– como uno de los líderes del debate internacional sobre las políticas de gobernanza de internet no resulta sorprendente ni novedoso si se considera, más allá de su dimensión geopolítica y sus diversas estrategias diplomáticas (incluyendo la del "poder blando"), la trayectoria interna desarrollada por sus actores en materia de políticas de internet en las últimas dos décadas.

El liderazgo de Brasil se debe tanto a su forma de abordar la gobernanza de internet en el plano interno, a partir de un mecanismo de múltiples actores que integran el CGI, creado en 1995, que lo ha transformado en un organismo de referencia en el país e internacionalmente, como al modelo asociado a la

[2] Agencia Nacional de Seguridad de los Estados Unidos. Este organismo utilizó un programa llamado PRISM que controló millones de datos informativos de gobiernos y ciudadanos del mundo.

gestión de los recursos de internet.[3] Entre otros resultados, este mecanismo le permitió facilitar respuestas coordinadas del Gobierno y los demás actores involucrados (sociedad civil, empresas y universidades) ante una amenaza externa a la gobernanza de internet, como lo fueron las acciones perpetuados por la NSA. A su vez, le permite coordinador procesos como el Marco Civil de Internet, iniciado en 2009 para impulsar una plataforma básica de principios para el uso y la gobernanza de internet. En la reglamentación del Marco Civil que culminó en 2016, el CGI ha sido designado como el organismo que debe supervisar la implementación de esta ley.[4]

Sin embargo, desde fines de 2012 emergieron diversas iniciativas en América Latina y el Caribe que toman en consideración las políticas y la gobernanza de internet como eje principal de trabajo, al igual que el CGI. Además de Brasil, en los siguientes países se encuentran desarrollos más recientes de algún tipo mecanismo a nivel nacional: Argentina, Colombia, Costa Rica, México, Paraguay, Perú, República Dominicana, Uruguay y Venezuela. La emergencia de la gobernanza de internet en las agendas políticas en diversos países de América Latina plantea diversas interrogantes que este trabajo busca responder: ¿Cuáles son los componentes institucionales? ¿Qué actores se encuentran representados y de qué manera? ¿Qué objetivos persiguen y cuáles han sido sus resultados? ¿En qué medida se encuentran replicados otros modelos institucionales? ¿Cómo se articulan estas iniciativas con otros espacios de diálogo internacional y regional?

Una premisa fundamental del trabajo es que estos mecanismos se constituyeron sobre la base de redes de políticas (*policy networks*), definidas como "patrones más o menos estables de relaciones sociales entre actores interdependientes, que se congregan en torno a problemas y/o programas políticos".[5] La imagen de una de *policy network* es la de un espacio de intercambio frecuente y de comunicación entre actores que lleva al desarrollo de relaciones estables

[3] Estos son los nombres de dominio, direcciones IP, la coordinación de los IXP, entre otras actividades.

[4] Este creciente protagonismo del CGI se encuentra cuestionado por el gobierno de transición del presidente Temer y por las operadoras de telecomunicaciones, lo que refuerza la relevancia que asumió este organismo en lo referente a las políticas y desarrollo de internet en el país en tanto amenaza a otros intereses económicos y políticos que son cuestionados por un diseño más descentralizado y abierto como el de internet.

[5] Traducción propia del inglés. Kikert, 1997, p. 6 (*citado en:* Blanco, I., Lowndes, V. y Pratchett, L., *Re-Organising Babylon: on the Meaning of Policy Networks and Network Governance and their Democratic Consequences*, paper preparado para la conferencia "Governance Networks: Democracy, Policy Innovation and Global Regulation", Roskilde, Roskilde University, diciembre 2-4, 2009, p. 6).

entre ellos. Para algunos autores esto conlleva a la coordinación mutua de intereses sobre dominios específicos de políticas.[6] Sin embargo, con el paso del tiempo estas redes de políticas para el campo de internet se vuelven cada vez más en "redes de gobernanza" que, a nivel institucional, emergen como resultado de incentivos específicos y tienden a formalizarse.[7]

A su vez, Peters[8] identifica cuatro mecanismos de gobernanza, que caracteriza como "sombras", para describir la autoridad existente por detrás de cada una de estas variantes de las redes de gobernanza emergentes en la actualidad. Estos son las "jerarquías", entendidas como el aparato estatal burocrático; los "mercados", mecanismo centrado en el poder de las grandes empresas o fuerzas de mercado (como el narcotráfico); la "sociedad", definida como las redes de actores sociales provenientes de la sociedad civil, y un cuarto, identificado como el "conocimiento" de los expertos (vinculado con el concepto de "comunidades epistémicas").[9]

El trabajo estará estructurado en tres partes. En la primera se caracteriza a la gobernanza de internet así como los fundamentos y principios que sustentan los procesos nacionales en esta materia. La segunda parte desarrolla el proceso de seis casos nacionales (Argentina, Colombia, Costa Rica, México, Uruguay y Venezuela) con el trasfondo del CGI de Brasil. Este último ha sido extensamente analizado, pero se utilizará como marco de referencia en tanto fue el primer proceso nacional diseñado para la gobernanza y las políticas nacionales vinculadas a internet desde 1995. Finalmente, en la última parte se brinda un análisis comparado y recomendaciones.

I. Caracterizando a la gobernanza de internet

La gobernanza de internet es un concepto esquivo, que se ha caracterizado como "una mancha del test de Rorschach",[10] ya que en las apreciaciones que

[6] Adam, S., y H. Kriesi, "The Network Approach", en P. A. Sabatier (ed.), *Theories of The Policy Process*, Boulder, Colorado: Westview Press, 2007.

[7] Blanco, Lowndes y Pratchett, *supra* nota 5, 2009.

[8] Peters, G., *Governing in the Shadows*, SFB-Governance Lecture Series, Nº. 3, DFG Research Center (SFB) 700, Berlín, 2010. Disponible en: http://bit.ly/2ejlPum

[9] De acuerdo a Haas (Haas, P. M. (1992), "Introduction: Epistemic Communities and International Policy Coordination", en *International Organization*, 46(1).), una comunidad epistémica es una red de profesionales con reconocida experiencia y competencia en un terreno particular de políticas o de temas. A pesar de que dichas comunidades pueden abarcar una variedad de disciplinas y entornos, comparten una serie de atributos: principios, normas y creencias, nociones de validez y de causalidad y objetivos de las políticas.

[10] Drake, William J., "Reframing Internet Governance Discourse: Fifteen Baseline Propositions", p. 1. Paper basado en presentaciones del *Workshop on Internet Governance*,

de ella hacen los distintos actores se expresan sus propias motivaciones y expectativas. Si bien existe cierto consenso a partir de la Cumbre Mundial de la Sociedad de Información (CMSI) y la Agenda de Túnez (2005), continúa siendo una cuestión ambigua y problemática: "El desarrollo y aplicación de los gobiernos, el sector privado, la sociedad civil, en sus respectivos roles, de principios, normas, reglas y procedimientos que moldean la evolución y el uso de internet". Esta definición de gobernanza de internet se emparenta con la definición de régimen en las relaciones internacionales como "un conjunto de principios (implícitos o explícitos), normas, reglas y procedimientos en los que convergen las expectativas de los actores en las relaciones internacionales",[11] que a su vez acompaña el giro institucionalista adoptado por esa disciplina.

La definición de gobernanza de internet de la CMSI ha tenido una influencia notoria en el marco de las políticas internacionales, pero tiene un carácter más normativo, y descriptivo, que analítico. No permite dar cuenta del proceso emergente que se ha caracterizado por el desarrollo de esta tecnología por parte de comunidades específicas, en las que dicho desarrollo y los usos de la tecnología determinan o, por lo menos, condicionan esos roles, principios y normas. Este segundo enfoque de la gobernanza estaría más emparentado con la perspectiva sociotécnica.

Pero más allá de las definiciones, las investigaciones relacionadas con la gobernanza de internet se han centrado en la dimensión global del problema, y en la conformación del régimen internacional, entendido como los "acuerdos dominantes".[12] Es cierto que internet es una tecnología sin fronteras, pero la dimensión mundial eclipsa las diferentes orientaciones de las dinámicas nacionales y las diversas capacidades desplegadas por actores en sus territorios en más de dos décadas desde la expansión de internet. La complejidad de internet requiere un gran conocimiento sobre su funcionamiento y sofisticadas estrategias de gobernanza por parte de los actores involucrados. Este argumento incorpora a los expertos en estrategias y políticas sobre el tema, para quienes son los conocimientos científico-técnicos los que fundamentan las decisiones, por ejemplo, desde la dimensión de la

International Telecommunication Union, Ginebra, febrero de 2004, y *United Nations ICT Task Force Global Forum on Internet Governance*, Nueva York, marzo de 2004.

[11] Krasner, Stephen, *International Regimes*, Palo Alto, Stanford University, 1983. Traducción propia.

[12] Keohane, Robert y Nye, Joseph S., *Power and Interdependence: World Politics in Transition*, Boston, Little, Brown and Company, 1989.

tecnocracia[13] y/o la gobernanza de los expertos.[14]

Además de aproximarse a la problemática de internet desde el punto de vista de los actores y acuerdos internacionales, otra posibilidad es hacerlo mediante el reconocimiento del grado de imbricación entre los aspectos técnicos y políticos de esta tecnología.[15] Los argumentos sociotécnicos clásicos como el de Bijker[16] sostienen que las decisiones técnicas están insertas en el contexto socioinstitucional en el que fueron creadas, e imbuidas de él. En esta línea, el proceso de la CMSI (2003-2005) cuestionó abiertamente la legitimidad institucional de los acuerdos iniciales de gobernanza que estaban descontextualizados y alejados de los intereses de los actores de países que no intervinieron en el desarrollo inicial de esta tecnología. Enfatizó las implicancias políticas de las decisiones que se desarrollaban en espacios como la Internet Corporation for Assigned Names and Numbers (ICANN) y otras reuniones de carácter técnico. La CMSI trajo al frente debates sobre el diseño institucional y los roles asignados a los distintos actores en la gobernanza de internet, incluyendo el reconocimiento de la gobernanza multiactor como un principio fundamental para todos los procesos. Utilizando la caracterización de Jupille y Snidal,[17] la CMSI abrió las puertas a los debates sobre "uso", "selección", "reformulación" y "cambio" en los arreglos institucionales existentes. La CMSI también amplió el debate sobre la agenda de gobernanza para trascender asuntos técnicos e institucionales de internet, e incluyó los temas vinculados a los derechos humanos y la dimensión de desarrollo. Es por este motivo que la agenda de gobernanza de internet en la actualidad es muy diversa y requiere de la participación de distintos especialistas y sectores para abarcar este espectro temático.

La necesidad de delimitar el campo y el foco de las políticas nacionales –aun cuando las mismas se encontraran en una fase emergente– ya había

[13] Centeno, Miguel Angel y Wolfson, Leandro, "Redefiniendo la tecnocracia", en: *Desarrollo Económico*, No. 37(146), 1997, pp. 215-240.

[14] Hall, Peter A., "Politics as a Process Structured in Space and Time", reunión anual de la American Political Science Association, Washington D.C., 2010.

[15] Drake, *supra* nota 10; Solum, Lawrence B., "Models of Internet Governance", en: Illinois Public Law Research Paper Nº 07-25, Illinois, 3rd September, 2008, p. 48-91; DeNardis, Laura, *The Global War for Internet Governance*, New Haven, Yale University Press, 2014.

[16] Bijker, W. E., "Sociohistorical technology studies", en S. Jasanoff, G. E. Marsh, J. C. Petersen, & T. Pinch (Eds.), *Handbook of Science and Technology Studies*, Sage Thousand Oaks, 1995.

[17] Jupille, J. y Snidal, D., "The Choice of International Institutions: Cooperation, Alternatives and Strategies", en: *American Political Science Association annual meeting*, Washington, D.C., septiembre de 2005.

aparecido durante la expansión de internet, con la delegación de nombres de dominio de primer nivel y de bloques de direcciones IP en la segunda mitad de la década de 1980 y comienzos de los 90. El desarrollo de capacidades locales en relación con internet, así como de mecanismos estables de coordinación nacional y de participación en los foros internacionales, también marcó las responsabilidades de actores nacionales provenientes de los sectores público, privado y científico.

Es de destacar que la inclusión de los países en desarrollo en los mecanismos de gobernanza de internet fue señalada en su momento por el Grupo de Trabajo para la Gobernanza de Internet (WGIG por sus siglas en inglés) y por otros como de vital importancia para garantizar el avance y la legitimidad del proceso.[18] Además, estos autores enfatizan una mayor creación de mecanismos nacionales de participación como condición previa para una actuación relevante en los foros internacionales. El WGIG brinda, además, una consideración relevante para el presente trabajo, y es que destaca cuatro recomendaciones sobre los mecanismos de gobernanza de internet: la función de foro, la supervisión de políticas públicas globales, la coordinación institucional entre organismos y la coordinación regional y nacional.

Kaul, Grunberg y Stern[19] distinguen tres brechas que presentan desafíos para la implementación de políticas públicas tendientes a la provisión de bienes públicos globales. Estas brechas, que dieron origen a las preocupaciones de legitimidad y representatividad de los procesos de gobernanza de internet de la última década, son las siguientes: a) una jurisdiccional, que se manifiesta en la discrepancia entre el crecimiento de los desafíos para las políticas globales, y los límites nacionales de las políticas públicas de los países; b) una brecha en la participación, derivada del hecho de que, a pesar de la creciente institucionalización de la intervención de otros actores no estatales en la cooperación internacional, estos tienen problemas de representación y legitimidad en muchos foros internacionales, especialmente cuando provienen de países menos desarrollados. Para los autores, la ventaja de incluir a esos actores sería que, al darles mayor participación, los Gobiernos podrían obtener mayor respaldo para sus decisiones políticas y, también, fomentar el

[18] Siganga, Waudo, "The Case for National Internet Governance Mechanisms", en: Drake, W.J. (ed.), *Reforming Internet Governance: Perspectives from the Working Group of Internet Governance (WGIG),* Nueva York, The United Nations Information and Communication Technologies Task Force, 2005; Afonso, C.A., *Gobernanza de Internet: un análisis en el contexto de la CMS*I, Montevideo, ITeM, 2005; Drake, supra nota 10.

[19] Kaul, I., Grunberg, I., & Stern, M. A., *Global public goods: international cooperation in the 21st century*, Oxford University Press, 1999.

pluralismo y la diversidad. Este es el argumento a favor de los procesos de participación multiactor (*multistakeholder*) de buena parte de los procesos de gobernanza de internet, y c) una brecha de incentivos, para controlar los efectos de las acciones de los países sobre los bienes públicos en la esfera internacional, no alcanza con incentivos de carácter moral. Hasta recientemente, y en particular por los efectos que han tenido en los últimos años los "escándalos" de internet, eran pocos los actores nacionales que percibían el tema como una necesidad o un problema, ya que los foros mundiales y los espacios de concreción de políticas internacionales aparecían lejanos en sus prioridades. Los mecanismos nacionales que se examinarán a continuación resultan ejemplos que permiten acortar parcialmente estas brechas.

En el ámbito nacional, hasta hace pocos años existían pocos países con mecanismos establecidos para el desarrollo de políticas de internet. Esto no significa que no existe una larga trayectoria de involucramiento incipiente en la temática así como de regulación en diversos aspectos (vinculados a la capa de contenidos y de infraestructura fundamentalmente). Pero los espacios específicos para el desarrollo de políticas de internet se encontraban menos definidos.

II. Gobernanza de internet: casos nacionales en América Latina

A continuación, se desarrollan los casos de estudio seleccionados. En cada uno se recurre a contextualizar la trayectoria de internet en el país desde sus orígenes, en tanto empíricamente se puede constatar que en muchos de ellos, especialmente en Brasil, Costa Rica, México y Uruguay, los pioneros en introducir y operar esta tecnología se encuentran involucrados en estos nuevos mecanismos emergentes.

II.A. Argentina

Como buena parte de los países de América Latina y de Europa, Argentina comenzó con sus actividades vinculadas a las redes informáticas como corolario de la introducción de internet en centros académicos y de investigación. En términos de adopción de protocolos de internet, para 1991 Argentina estaba conectada a las mayores redes internacionales, dentro de las cuales internet era una de ellas pero no la única.[20] Sin embargo, la expansión de internet recién comenzó a cobrar impulso una vez que se liberalizó el mercado de las

[20] Otras redes conocidas y en competencia con la internet en aquel entonces eran BITNET, UUCP y Usenet.

comunicaciones internacionales en 1997. Hasta entonces, y si bien el mercado de las telecomunicaciones se abrió en 1990, la situación real era de oligopolio en el mercado interno, y de monopolio a través de la sociedad TELINTAR, formada por TELECOM y Telefónica para el enlace internacional.

Los esfuerzos de los llamados "pioneros de internet" para lograr conectividad al enlace internacional a un precio accesible fue una dura batalla que fue muy influyente en la definición de lo que podría considerarse el "espíritu de internet" de varios de estos nuevos actores emergentes. Estos se podían ubicar entre aquellos provenientes del ámbito académico, como el Departamento de Computación en la Facultad de Ciencias Exactas y Naturales de la UBA, la red académica RETINA, o los actores vinculados al emergente sector privado de emprendedores que se distinguían de los proveedores de telecomunicaciones y se agruparon en 1989 en CABASE, la cámara del incipiente sector.

En términos de relaciones con los procesos internacionales, no fue sino hasta el proceso de la CMSI en 2003 que los actores gubernamentales mostraron una actitud más proactiva al régimen internacional de internet. La agenda política de internet se enfocó en los aspectos de despliegue y adopción de nuevas tecnologías, incluyendo los temas de pobreza y la brecha socioeconómica, más que en los aspectos políticos del régimen internacional. Esto, sin embargo, comenzó a cambiar desde Túnez. Allí Argentina envió una gran delegación a la CMSI y tuvo, en términos regionales, un alto perfil en la conferencia. Pero esta reunión tuvo poco impacto en los mecanismos institucionales y en las políticas internas, a excepción de haber logrado posicionar en algunos sectores del Estado, particularmente en Cancillería, la necesidad de dar seguimiento a estos temas. Los actores involucrados en las distintas capas de políticas de internet en el país todavía basaban sus acciones en mecanismos de coordinación informal, sobre la base de años de trabajo conjunto.

En los últimos cinco años, ha habido cambios que emergen de una visión particular acerca del rol del Estado en muchas áreas de política en el país, en especial en aquellos sectores que involucran a bienes y servicios públicos, donde el Estado interviene no solo a través de la regulación, pero también como proveedor de servicios en el sector de las comunicaciones. Algunos de los ejemplos que ilustran esta posición son el Plan Nacional Argentina Conectada de 2010, en el cual se ampliaron las redes troncales del país con inversión pública en una red de fibra óptica. Otro ejemplo es el de ARSAT, una empresa creada por el Estado en 2006 para desarrollar servicios de comunicación satelital. Con la digitalización del espectro y el desarrollo del Plan Argentina Conectada, ARSAT ha quedado en una posición de proveedor de servicios de telecomunicaciones. El último ejemplo

proviene tanto del papel que tuvo la Ley Argentina Digital, aprobada en el Congreso en diciembre de 2014 y parcialmente derogada con el nuevo gobierno en diciembre de 2015, así como por la creación del Ministerio de Comunicaciones, siguiendo la experiencia colombiana en esta materia que se analizará más adelante. Este ministerio absorbe las distintas funciones de comunicaciones diseminadas en diversas dependencias, a la vez que el mismo decreto que lo crea (267/15) es el que origina al nuevo ente regulador, Ente Nacional de Comunicaciones (ENACOM). Más allá de las diferencias entre un proyecto, como el de Argentina Digital y su entre de aplicación y regulación llamado AFTIC, y la propuesta actual de creación de un Ministerio de Comunicaciones y ENACOM, cabe destacar que se mantiene presente una línea de creciente intervención e interés del Estado por esta temática que se puede identificar a abril de 2014 cuando se convocó a la corta experiencia de la Comisión Argentina de Políticas de Internet (CAPI)[21] por la Secretaría de Comunicaciones. Pero es prematuro adentrarse en un análisis en esta línea, y sus implicancias para internet y su gobernanza, considerando el poco tiempo transcurrido y que aún no se ha divulgado la Ley de Convergencia anunciada para enmarcar jurídicamente el proceso.

Más específicamente para el caso de la gobernanza de internet en este país, con el cambio de gobierno a fines de 2015 se creó un Ministerio de Modernización que contempla la temática en varias de sus dependencias, y en la Secretaría de Innovación y Gestión Pública se crea la Dirección Nacional de Políticas y Desarrollo de Internet[22] cuyos objetivos incluyen la representación del Estado nacional en ámbitos internacionales vinculados con la temática, y el diseño y desarrollo de políticas de gobernanza de internet en el territorio nacional. De esta manera, el tema queda instalado en la agenda pública nacional y se institucionaliza dentro del Estado, pero siguiendo un formato clásico de consolidación de un área dentro de una burocracia. Al igual que con el nuevo Ministerio de Comunicaciones y ente regulador (ENACOM), es aún prematuro considerar los efectos de esta secretaría y dirección nacional sobre los mecanismos nacionales de gobernanza con otros actores no gubernamentales.

[21] Esta fue una comisión creada mediante una resolución (Res. SECOOM 13/2014) integrada por entidades gubernamentales con el objetivo primario de mayor coordinación intra-Estado, que si bien tuvo intenciones de inaugurar un proceso de gobernanza multiparticipativa, la propia Ley Argentina Digital terminó de invalidar este intento.

[22] Las subsecretarías dependientes del Ministerio de Modernización se crearon por la Decisión Administrativa 232/2016 el 29 de marzo de 2016. Disponible en: http://bit.ly/1pKRENB.

Por último, el caso argentino reporta un proceso incipiente de foro nacional de gobernanza de internet con la creación del primer Diálogo Argentino para la Gobernanza de Internet realizado el 27 de octubre de 2015. Este mecanismo se consolidó a partir de la participación de distintos actores –sociedad civil, gobierno, comunidad técnica y empresas– en el ámbito de listas de discusión electrónica y encuentros para discutir temas candentes regulatorios y políticos en materia de internet y nuevas tecnologías. La generación de vínculos informales a partir de estos espacios de interacción entre algunos actores, que además venían participando de procesos internacionales y reuniones en el marco de ICANN, Internet Governance Forum (IGF), Foro de Gobernanza de Internet de América Latina y el Caribe (LACIGF), LACNIC y CMSI inspiró al grupo a organizar foro nacional, siguiendo las experiencias de otros espacios regionales, notoriamente del Grupo Iniciativa en México, que se analizará más adelante, y que ya ha organizado dos Diálogos Mexicanos de Gobernanza de Internet.

La forma institucional que asumió el grupo organizador del Diálogo en Argentina es la de un comité multisectorial con presencia de todas las partes interesadas en el sentido tradicional de la gobernanza de internet, compuesto por nueve personas de los distintos sectores.[23] El grupo organizador abrió un llamado a participantes para conformar un comité de agenda para el primer evento. Para ello se convocó a una reunión abierta en la que se definieron los ejes temáticos a partir de los cuales hubo un período de comentarios públicos desde un formulario en la web del evento para terminar de definir la agenda. El diálogo contó con presencia de actores de todos los sectores y constituyó una primera experiencia que volverá a ser replicada en 2016, esta vez con un formato más formalizado y se llamará "IGF Argentina".[24] Una de las principales consecuencias de este Diálogo fue materializar la presencia del tema en la agenda pública, que fue retomada por varios de los actores participantes que luego de las elecciones pasaron a integrar cargos de gestión nacional donde actualmente se están consolidando estos temas como se presentó en el caso del Ministerio de Modernización.

A modo de síntesis, desde abril de 2014 y la participación argentina en Netmundial, la gobernanza de internet en Argentina se ha transformado, a través de distintos mecanismos (muchos de ellos de corta duración), en una

[23] Una de las integrantes que representa al sector académico en la discusión es la propia autora de este trabajo.

[24] Al momento de terminar este trabajo en julio de 2016, el grupo organizador del Diálogo convocó a una reunión preparatoria para el IGF Argentina el 19 de julio, en el que se establecerá un comité de programa seleccionado por integrantes de los distintos sectores.

prioridad más clara para el Estado. Los demás actores que históricamente han realizado gobernanza *de facto* de internet por el hecho de ser operadores de recursos, tecnologías y estándares en el país continúan consolidando sus acciones, y la primera edición del Diálogo en 2015 constituye una señal clara, que acompaña la definición de una *policy network*. Pero lo más notable en términos de mecanismos institucionales más recientes en el país le corresponde a la interpretación realizada desde el Estado de la necesidad de generar mayor coordinación y promover el conocimiento, para poder intervenir con mayor efectividad en este entorno.

II.B. Costa Rica

Costa Rica presenta un panorama con una tradición de iniciativas de interconexión a las redes, siendo el primer país centroamericano en conectarse a internet en 1993. Estos esfuerzos eran el resultado de emprendimientos científicos y de dos organizaciones involucradas en el desarrollo de la infraestructura de internet y de las telecomunicaciones en ese país, RACSA e ICE. Institucionalmente, esos emprendimientos comenzaron en la Universidad de Costa Rica, que estuvo involucrada con otras universidades centroamericanas en el desarrollo de una red regional.[25] Adicionalmente, Costa Rica fue el primer país de la región en desarrollar una red troncal exclusiva para IP en 1993 y fue uno de los pocos en América Latina cuyos sistemas de telecomunicaciones permanecieron bajo la órbita del Estado (el ICE fue monopolio estatal hasta el 2008). Esta última característica, sumada al desarrollo de tecnología propia en el marco de los centros de investigación de las universidades, permitió un despliegue de internet independiente de los intereses de los grandes grupos internacionales.[26] Aun culminado el monopolio estatal en las telecomunicaciones, la presencia del sector gubernamental en ese país ha seguido vigente en los temas de internet, como se verá a continuación con el desarrollo de mecanismos específicos nacionales para el desarrollo de políticas de internet.

En 2012, Costa Rica fue el organizador de la reunión ICANN 43. En la inauguración de esta reunión, la entonces presidente Laura Chinchilla proclamó un discurso que no solo apuntaba a mejorar las características de la internet en su país, sino además a mejorar las características del entorno

[25] Siles González, Ignacio, *Por un sueño en.re.dado. Una historia de internet en Costa Rica (1990-2005)*, Montes de Oca, UCR, Instituto de Investigaciones Sociales, 2008.

[26] Téramond, G.F., *Interconexión de Costa Rica a las grandes redes de investigación Bitnet e internet. Ideario de la ciencia y la tecnología: hacia el nuevo milenio*, San José, Ministerio de Ciencia y Tecnología, 1994, disponible en: http://bit.ly/2fDHbz2

digital global. Ese mismo año, se creó el Consejo Consultivo de Internet (CCI) de Costa Rica organizado por el "nic.cr". Este organismo (administrador del punto de dominio ".cr") es parte de la Academia Nacional de Ciencias de ese país y ambas organizaciones han tenido una larga trayectoria de involucramiento en el desarrollo de internet en Costa Rica. El CCI fue convocado a iniciativa del ".cr" y con el paraguas organizacional que este tiene para crear una plataforma para la discusión sobre los aspectos más relevantes para el desarrollo de internet en ese país. Algunos de los temas que aborda son: plan nacional de banda ancha, Fondo de Acceso Universal, y el desarrollo del primer IXP establecido en 2014. Sus objetivos formales son participar en las recomendaciones de política para el "nic.cr" y el despliegue de internet para el cumplimiento de objetivos de desarrollo del país.

En cuanto a la composición del CCI, si bien es un órgano multiactor, con representantes de agencias gubernamentales, instituciones científicas, ONG y empresas, la mayoría de sus miembros son entidades gubernamentales y estatales. De esta manera, si bien el principio de múltiples partes interesadas se encuentra en la base de sus prácticas operativas, el CCI tiene una orientación hacia el sector gubernamental.

Si bien el CCI no produce documentos formales, ni establece posiciones a nivel nacional sobre una temática –como es claramente el caso del Comitê Gestor de Internet do Brasil "CGI.br"– es una plataforma de discusión y de validación de iniciativas, sobre todo lideradas por el ".cr" en la dimensión técnica. En cuanto a la modalidad de trabajo, la mayor parte de las reuniones se produce en formato online en los distintos grupos de trabajo que componen el CCI: políticas nacionales de internet, seguridad de internet, red educativa, cibercrimen, infraestructura y promoción del dominio ".cr", aunque se producen reuniones presenciales en forma semestral.

El "nic.cr" analizó previamente la experiencia llevada adelante por los registros nacionales de dominio de México (".mx") y con el "CGI.br" y su brazo operativo, el "nic.br", antes de convocar a la formación del CCI. Este último es bastante menos formal que la experiencia brasileña y a diferencia de la experiencia en México, que se analizará más adelante, la participación es por instituciones y no por personas. De acuerdo a la experiencia de participación en este cuerpo por parte de un representante de la SUTEL (el regulador), de haber existido mecanismos más formales se hubieran generado tensiones con los organismos que actualmente no forman parte del mismo. El potencial de apertura hacia nuevos actores es una dimensión relevante, en tanto aquellos actores que actualmente no forman parte de este organismo podrían cuestionar su legitimidad.

Con respecto a su foco y objetivos, existen diversas opiniones dependiendo de si los actores son o no de gobierno. Para estos últimos, el CCI constituye un espacio informal de aprendizaje, experiencias compartidas y de recepción de insumos para el desarrollo de políticas. Para los otros actores, este constituye efectivamente un espacio de gobernanza.

La experiencia del CCI en Costa Rica ejemplifica un esfuerzo de formalización de una *policy network* para la producción de resultados concretos en aspectos técnicos de la gobernanza de internet que ya han dado resultados concretos, como el informe de dominios ".cr", el lanzamiento del primer IXP en 2014 y el desarrollo de módulos de capacitación en ciberseguridad. A pesar de la naturaleza no-vinculante de este organismo, la participación del gobierno en esta iniciativa constituye una validación de otros mecanismos para el desarrollo de políticas y gobernanza de internet en ese país.

II.C. Colombia

Al igual que en otros países de la región, los orígenes de internet en Colombia están relacionados con el ámbito académico. En 1991 Jon Postel –entonces administrador de la Internet Assigned Numbers Authority (IANA)– delega la administración del dominio colombiano a la Universidad de los Andes. También, al igual que otros países de la región, en la década de 1990 se inició el proceso de liberalización del mercado de las telecomunicaciones, hasta entonces operado por un solo actor gubernamental y su empresa nacional de telecomunicaciones, TELECOM.

Pero a diferencia de otros casos regionales, en Colombia existe una visión convergente de las comunicaciones aun previamente a la era digital, ya que desde 1953 se creó el Ministerio de Comunicaciones aglutinando los temas de correos, telecomunicaciones y giros. Desde entonces, y en particular con el desarrollo de internet en el país que tuvo su explosión para 1998-1999, el Ministerio comenzó a intervenir para favorecer la adopción de internet entre sus ciudadanos. Este ministerio finalmente cambió de nombre en 2009 bajo la Ley 1.341 para pasar a denominarse Ministerio de Tecnologías de la Información y las Comunicaciones. El objetivo de esta ley es la creación de un marco normativo para el desarrollo del sector, masificar el uso de las TIC, impulsar la competencia y fortalecer la protección de los derechos de los usuarios.

Un aspecto característico de los inicios de internet en Colombia fue el largo proceso entre 2002 y 2009 en el cual el Ministerio de Comunicaciones, y luego MINTIC, pasó a regular el registro de código de país hasta que finalmente la operación del dominio fue traspasada de la Universidad de los Andes

a la empresa CO Internet SAS, bajo la tutela del ministerio. Este hecho, al igual que en otros casos regionales donde existió una pugna por recursos de internet, tuvo consecuencias importantes para la instauración de un proceso de gobernanza nacional por la toma de conciencia e interés específico en el asunto, delimitando de esta forma un campo temático y político específico.

La realización de la quinta edición del LACIGF en Bogotá en el año 2011 llevó al comienzo de las interacciones de un diverso grupo de actores del país trabajando sobre el tema. Los actores que integraban esta plataforma informal de diálogo lo hacían motivados para intercambiar sus perspectivas previas de un evento, o en torno a un tema específico de relevancia. El grupo "Mesa Colombiana para la Gobernanza de Internet" se planteó bajo un formato multiactor con representantes de sociedad civil, gobierno, academia, comunidad técnica y sector privado en el sexto LACIGF de Córdoba. Desde entonces, el grupo organizó reuniones periódicas, de manera informal, hasta que se realizó el primer foro de gobernanza de internet de Colombia en noviembre de 2014 en la Universidad Javeriana de Bogotá y la segunda en septiembre de 2015 en el Hotel Tequendama de la misma ciudad.

La Mesa Colombiana de Gobernanza de Internet es un espacio abierto a la participación de más actores, aunque tiene un núcleo que funciona como secretaría estable y una nómina de participantes, también estables, que representan al sector académico, privado (cinco), gubernamental (dos) y a la sociedad civil (seis). Sin embargo, si bien el sector académico tiene un espacio destinado a sus representantes, la participación de este actor se encuentra rezagada por falta de incentivos propios, aun cuando se registran participantes a sus reuniones. Es notoria la integración de actores pioneros de internet en esta mesa, como representantes de varios de los sectores, lo que remite a la metáfora de una red de políticas, en vías de consolidar una red de gobernanza. Atendiendo a su formato de trabajo, tiene cinco ejes temáticos (internet para la reducción de la pobreza, neutralidad, gobernanza de internet, ciberseguridad y ciberdefensa, y libertad de expresión) que estructuran su agenda, aunque también se analizan temas de actualidad. Los mecanismos de coordinación y diálogo dentro del grupo son multiplataforma (listas de correo, teleconferencias, etherpad) además de las reuniones bimestrales presenciales para las que se elaboran actas. Esta modalidad de trabajo por áreas, sumado a la posibilidad de interacción constante y a la producción de documentos específicos en relación a las distintas temáticas que atiende la Mesa constituye uno de los productos más relevantes de esta iniciativa.

Tanto por la apertura, la posibilidad de participación de las múltiples partes interesadas en pie de igualdad y por el desarrollo de la agenda de

trabajo que se va generando, la experiencia de la Mesa Colombiana se encuentra alineada con varios de los principios esbozados en el marco de la CMSI y el IGF, así como por metodologías de trabajo visibles en otros organismos como ICANN o la Internet Engineering Task Force (IETF). Esta coordinación con otros espacios regionales –como fue el caso de los inicios de este proceso en el marco del LACIGF, como de la esfera internacional- se produce a través de la propia participación de estos actores en esas instancias.

II.D. México

A comienzos de la década de 1990, la infraestructura de redes para internet en México representaba uno de los mejores escenarios regionales, en el que tres redes académicas brindaban servicios a sus usuarios en tres de las mayores zonas pobladas del país. Estos esfuerzos contaron inicialmente con apoyo gubernamental, pero a medida que avanzaban comenzaron también a duplicar esfuerzos y a competir por el financiamiento.[27] Había varios actores vinculados con infraestructura básica de internet entonces: por un lado, estaba el ".mx", que había sido delegado por Jon Postel al ITESM[28] en 1989, por otro, la red de la UNAM[29] administraba un bloque tipo B de direcciones IP,[30] y por otra parte, estaba la Red Tecnológica Nacional. El capítulo Internet Society (ISOC) México trabajaba en el contexto de la UNAM y existía un acuerdo tácito de división de los asuntos técnicos y los políticos entre estos dos centros universitarios mayores, el ITESM y la UNAM.

Para 1995, con el incremento en la popularidad de internet gracias a la aparición pública de la World Wide Web, se volvió indispensable integrar los esfuerzos. El ITESM se convirtió de esta forma en *country code Top Level Domain* (ccTLD) y en registro nacional de dirección de Internet en México (NIR).

Estos inicios atravesados por rivalidades en la coordinación de recursos e infraestructura básica de internet dejó un legado importante a los pioneros de internet en ambas universidades. Interpretaron que debían trabajar en consonancia con los marcos de acción desarrollados internacionalmente en el incipiente régimen tanto para comprender estas reglas, pero también para

[27] Gayosso, Blanca, "Cómo se conectó México a la Internet. La experiencia de la UNAM", en: *Revista Digital Universitaria*, No. 4(3), Ciudad de México, 2003, disponible en: http://bit.ly/1x9AieR

[28] Instituto Tecnológico Superior de Monterrey.

[29] Universidad Nacional Autónoma de México.

[30] Esto es un bloque de 65.356 hosts, un número muy alto para una época donde internet todavía no había despegado masivamente a la ciudadanía.

modificar y crear nuevas instituciones y fortalecer su posición doméstica.

Mientras que estos ingenieros y pioneros de la internet en México desplegaban nuevos mecanismos institucionales para operar con estas nuevas tecnologías, las autoridades regulatorias de telecomunicaciones concentraron su energía en otros ámbitos. El surgimiento de Telmex como empresa privada fue producto de esta acción estatal y que conllevó como exigencia el desarrollo de una red de fibra óptica que despegó a México de otros países regionales en calidad de acceso a internet. Entre 1995 y 2006, se consolidó la Comisión Federal de Telecomunicaciones (COFETEL) como reguladora aunque su capacidad de acción era muy limitada, a pesar de una reforma en el año 2006. El demorado proceso de reforma de las telecomunicaciones en el sector culminó con la asunción del presidente Enrique Peña Nieto a fines de 2012, desde la cual surgieron varias líneas de acción del gobierno. Una primera medida fue la creación de la Agencia Estrategia Digital Nacional, cuyo objetivo es la coordinación de los asuntos de internet en las oficinas del Poder Ejecutivo, incluyendo aspectos de gobernanza de internet y de comunicación digital y la creación del Instituto Federal de Telecomunicaciones (IFT), que finalmente propuso un orden al sector. Antes de continuar con el impacto de la estrategia presidencial a partir de 2012, es fundamental destacar la iniciativa parlamentaria de 2009 mediante la cual se intentó gravar a los servicios de internet con un 3% de impuestos. La iniciativa no prosperó gracias a una masiva movilización virtual en Twitter y otras redes bajo el lema #InternetNecesario, a la vez que movilizó a personas en las calles en las principales ciudades. Esto aceleró el involucramiento de la sociedad civil y otros actores en la importancia de participar en la discusión de las políticas públicas en materia de internet.

La creación de la Estrategia Digital Nacional sacudió el entorno en tanto propuso cinco objetivos centrales para el desarrollo de la estrategia: transformación gubernamental, economía digital, educación de calidad, salud universal y efectiva, y seguridad ciudadana, que se cumplen con un entorno habilitador en el cual se incluye a la gobernanza de internet en el país. Esta estrategia resultó ser un detonante fundamental para que otros actores históricos de internet desarrollaran el Grupo Iniciativa, como los ya mencionados ("nic.mx", capítulo ISOC México, UNAM), así como la Asociación Mexicana de Internet (AMIPCI). Estos y otros ya eran un grupo informal, con débiles mecanismos formales de coordinación, pero que en la práctica eran una red de política sobre la base de años de confianza y lazos personales. Este no tenía estructura oficial, ni legal, y comenzó a operar en 2013, bajo el manto de conversaciones informales entre distintos sectores reunidos en una lista de correo electrónico. Inicialmente, el ".mx"

en su rol de organizador contactó a dos representantes de cinco sectores (academia, gobierno, comunidad técnica, empresas y sociedad civil) para conformar el grupo y adoptó los siguientes principios vinculados a los aspectos organizativos: participación equitativa, representación equilibrada, liderazgo automotivado más que formal, sobre la base del tema de discusión y decisiones basadas en el consenso.[31]

En 2013, el grupo accedió a producir insumos formales y decidió organizar una reunión que reflejara la naturaleza fluida e interactiva del trabajo del Grupo Iniciativa que se llamó "Diálogos Mexicanos para la Gobernanza de Internet", un evento con características de lo que se podría considerar como un IGF nacional. El programa fue desarrollado con insumos de encuestas a referentes de la comunidad de internet en México, y la temática refleja una variedad de asuntos que van de los derechos humanos, el comercio electrónico y la participación online. El evento tuvo una gran concurrencia, con más de ciento cincuenta participantes presenciales y tres mil dispositivos se conectaron a la plataforma online para el seguimiento remoto. En febrero de 2015, se realizó una segunda edición con similares niveles de participación y adhesión. Pero más allá de los Diálogos, el grupo mantiene una presencia e identidad a partir de su coordinación y discusión sobre temas de actualidad en el marco de su lista de correo.[32]

El Grupo se encuentra inspirado en principios generales de trabajo de la comunidad técnica de internet y sus mecanismos (IETF, ICANN) en su elección de discusión sobre discusiones basadas en el consenso, apertura, igualdad y el abordaje de la Agenda de Túnez hacia una gobernanza de internet basada en el respeto y la promoción de los derechos humanos.

Esta iniciativa ha resultado especialmente relevante durante la realización del LACIGF en la Ciudad de México en 2015, en tanto sirvió como órgano interlocutor nacional en la formulación de la agenda regional. Tendrá además un papel que definir para sí con la realización del Foro de Gobernanza de Internet 2016 en Guadalajara a fin de año que pondrá en juego la validez de este mecanismo como puente entre la gobernanza nacional e internacional, a la vez que como *policy network* es el espacio que permite coordinar a los distintos actores nacionales.

[31] Entrevista realizada el 16 de julio de 2014 a Manuel Haces, gerente de prospectiva de Network Information Center México (NIC.MX) en el 7º LACIGF, El Salvador.

[32] El grupo de correo utilizado es grupodeiniciativa@nic.mx.

II.D. Uruguay y Venezuela: experiencias incipientes

Como se anticipó al comienzo, existen otras iniciativas nacionales en la región, pero que aún son emergentes. Una de ellas es el caso de Venezuela, que en 2014 y 2015 realizó sendas ediciones de un diálogo venezolano para la gobernanza de internet. La motivación fundamental para los organizadores de estos encuentros, que fue el capítulo de ISOC de ese país, fue habilitar un espacio multiactor para el diálogo. Considerando el contexto político en Venezuela, y el papel del gobierno en la esfera pública del país, no resultó una tarea fácil para los organizadores conformar un espacio de diálogo sobre temas complejos y polémicos, como suele ser la agenda de la gobernanza de internet. A pesar de las controversias y disputas en torno a los diversos temas que se trataron en el programa, que incluyeron reclamos y cuestionamientos entre los actores sobre temas de neutralidad de la red, derechos humanos en internet y políticas de acceso, el evento logró sentar una base de legitimidad para continuar operando y organizar un segundo foro. La segunda edición fue organizada conjuntamente por la Asociación de Usuarios y Usuarias de Internet (Internauta Venezuela) y el capítulo ISOC de Venezuela que titularon "II Encuentro sobre Gobernanza de Internet para el Desarrollo y la Transformación Social del Estado", realizado en el auditorio de CANTV. La segunda edición del evento contó con aún más participantes y mayor involucramiento del gobierno en los distintos paneles.

La instalación de este foro tiene similitudes con otros eventos regionales e internacionales de características similares, notoriamente el LACIGF o el IGF, desde los cuales los organizadores han basado los principios orientadores de estos espacios. Uno de los resultados más destacados de estos foros es que el gobierno de Venezuela a través de la Comisión Nacional de Telecomunicaciones (CONATEL) se encuentra al momento de la publicación de este trabajo desarrollando un proceso para instalar un modelo de múltiples partes interesadas desde el gobierno.

El caso de Uruguay posee puntos de contacto con la experiencia venezolana, ya que la iniciativa surge del capítulo de ISOC en ese país y tuvo como objetivo desarrollar el primer foro de gobernanza de internet realizado en mayo de 2016, bajo el lema "Internet en Uruguay: un diálogo entre todos". Hasta ahora se plantea únicamente como espacio de convergencia de los actores involucrados en la materia para la organización de los foros. Si bien esta era una idea que el gobierno de ese país, a través de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de

la Información y del Conocimiento (AGESIC),[33] buscaba se materializara en el contexto nacional, también tenía presente que no deberían ser ellos quienes lideraran la iniciativa para no imbuir al proceso de la lógica gubernamental. Al igual que en Costa Rica, la presencia histórica del Estado en las comunicaciones del país ha sido, y sigue siendo dominante por la estructura del sector entorno a un ente monopólico nacional (ANTEL). Los organizadores realizaron una convocatoria abierta a todos los organismos y personas interesados en sumarse a la iniciativa para desarrollar la agenda el evento. La participación de diversas organizaciones vinculadas a la Casa de Internet de América Latina y el Caribe con sede en Montevideo en el armado de esta agenda influyó en esta iniciativa, en tanto trajeron la experiencia de otros foros nacionales, y reuniones regionales e internacionales, lo que genera mecanismos de isomorfismo con otras experiencias. El foro contó con más de ciento cincuenta participantes presenciales y el doble en cantidad de dispositivos conectados remotamente. En definitiva, este caso muestra un avance sobre la consolidación de una red de políticas sobre el sector de internet en ese país.

II. Análisis comparado

Si bien los orígenes de los mecanismos iniciados son distintos, se pueden identificar una serie de coyunturas críticas,[34] entendidas como momentos de definición que promovieron el puntapié inicial. Algunas de ellas provinieron de factores externos, como es el caso de Argentina y Colombia, en otras el detonante fue interno, como en México y Costa Rica. En el caso de Argentina, la reunión Netmundial puso de manifiesto dentro del Estado la necesidad de actuar coordinadamente, y de generar mecanismos de diálogo con otros actores para llevar adelante el proceso. En Costa Rica el impulso que tomó la gobernanza de internet en la agenda presidencial fue aprovechado como una oportunidad para desarrollar el CCI. En Colombia la necesidad de coordinarse y entender las posiciones de los actores locales

[33] Es una agencia descentralizada que hace casi una década desarrolla la agenda digital del país que participa de los espacios internacionales relacionados con la gobernanza de internet.

[34] Entendidas como las decisiones tomadas que producen legados que se perpetúan en el tiempo, en un escenario donde predomina la contingencia y el accidente histórico (Capoccia, Giovanni y Kelemen, R.Daniel, "The Study of Critical Junctures: Theory, Narrative, and Counterfactuals", en: *Historical Institutionalism World Politics*, Vol. 59, Nº 3, Cambridge University Press, abril de 2007, pp. 341-369. Disponible en: http://bit.ly/2fSoFb0.

ante un evento regional como el LACIGF dentro del propio fue un factor clave para el despegue de la Mesa de Gobernanza. En México el impulso de un nuevo gobierno y la creación de una agencia especializada y transversal a las nuevas tecnologías motivaron a los demás actores involucrados en el desarrollo técnico y comercial de internet a desarrollar un mecanismo de múltiples partes interesadas. Los casos de Venezuela y Uruguay muestran un claro impulso y respaldo de la Internet Society a través de sus mecanismos de capítulo para el desarrollo de estas iniciativas.

En relación al alcance y a los objetivos de estas iniciativas, hay una variación considerable en los casos analizados. Salvo la experiencia del CGI, todas las iniciativas reflejadas en este documento son mecanismos muy recientes. Como el propio caso del CGI ha demostrado, el proceso de consolidar una iniciativa de características multipartitas requiere tiempo y compromiso con un proyecto que se consolida como un espacio de colaboración voluntaria, y que intenta trascender la red de políticas para transformarse en una red de gobernanza. El pasaje de una red de políticas a una red de gobernanza depende de las características de cada contexto, y no siempre es necesario. En algunos casos, si se percibe hostilidad o desconocimiento sobre los temas de gobernanza de internet, una red de políticas no es suficiente y se deberá fortalecer un mecanismo de red de gobernanza. Si algunas de estas experiencias logran consolidarse en el mediano plazo, como indicarían actualmente las experiencias de Costa Rica, Colombia y México, se podría fortalecer su capacidad institucional para desarrollarse en la línea de una red de gobernanza.

Paralelamente, estos procesos rehúyen a una formalización que ralentice los tiempos de trabajo, o que genere trabas burocráticas, lo que constituye un sello tradicional de la forma de avanzar sobre la agenda de internet propia de los mecanismos originales adoptados por los ingenieros de internet en torno a la IETF. A la vez, ninguno está facultado para emitir recomendaciones o propuestas de carácter vinculante, ni siquiera el CGI hasta muy recientemente. En muchos de estos casos, los procesos aparecen como recomendaciones, y la capacidad formal que surge de estos espacios es de carácter consultivo.

La principal fortaleza de estos mecanismos radica fundamentalmente en la construcción de legitimidad de un proceso, para el cual es necesario construir diálogos para informar a los hacedores de política e intercambiar perspectivas diversas, y encontradas. También en la capacidad de delimitar agendas. Pero es fundamental que los resultados obtenidos de estos intercambios y deliberaciones queden plasmados en forma documental u otro formato (audiovisual, por ejemplo), de manera tal de construir un legado y una memoria sobre mecanismos que de lo contrario aparecen

como efímeros o iniciativas aisladas. También es importante distinguir que estos espacios no tienen el mismo significado para todos los actores que participan en ellos. Más allá del interés, y la vocación de servicio y de interés público que muchos de los participantes manifiestan como motivación para su trabajo en estos espacios, tienen connotaciones e impacto distintivo dependiendo de cada sector y coyuntura.

Para los actores que participan de estas iniciativas, la formalización de estos espacios ha tenido algunas ventajas sustantivas. En primer término tienen acceso a información y conocimiento de forma más estable y organizada que les permite, en casos como el del "nic.cr" como organizador del CCI de Costa Rica, validar sus estrategias de desarrollo, o consolidar estrategias de carácter multiactor y nacionales ante eventos internacionales, como ha sido el caso del Grupo de Iniciativa en México y de la experiencia colombiana. En segundo lugar, se establecen parámetros más claros de agenda y de acción, que sin algún mecanismo formalizado (como sería en una red de políticas), quedarían disueltos. Sin embargo, en países con escasa trayectoria en materia de redes de gobernanza formalmente establecidas con actores no gubernamentales, como es el caso de buena parte de América Latina, la posibilidad que estos mecanismos adquieran alguna función adicional a la de constituirse en procesos consultivos, es una posibilidad que es rechazada, tanto por los representantes gubernamentales que participan de estas iniciativas, como por otros actores (aunque en este último caso se encuentran más matices en las posiciones).[35]

También hay que destacar que existen variaciones tanto en la composición de actores participantes de estas iniciativas, como en su nivel de participación. El caso argentino es aún incipiente y el cambio de gobierno en el que se incluye la agenda de la gobernanza de internet acrecentará su representación y participación en la incipiente Secretaría/Comité de Programa del IGF Argentina. En el caso del Grupo Iniciativa de México, si bien en los principios originales del grupo la idea era que hubiera dos representantes por sector, en la actualidad el grupo de actores de gobierno tiene más representantes que los demás, en parte debido a la introducción de los temas de la agenda de gobernanza en más organismos gubernamentales, tendencia que también se observa en los demás casos nacionales analizados. Cabe señalar que en el caso del CGI, que se utiliza como marco de referencia, el proceso

[35] En la propia literatura sobre redes de gobernanza hay posiciones muy críticas hacia ciertos mecanismos de gobernanza en red que son opacos y hasta pueden desafiar a las autoridades estatales.

de participación más equilibrada, con una mayor representación de los actores no gubernamentales se dio a partir de 2003, cuando con el Decreto 4.829 se realizó una reforma de estatutos que modificó la participación de los delegados de los distintos sectores, así como la creación de "nic.br", organismo que administra recursos de internet de Brasil.

Las experiencias analizadas en los casos nacionales también varían en el grado de adaptación/adopción a las reglas de juego globales de la gobernanza de internet. El CGI en Brasil, definido antes que muchos de los procesos e institucionales regionales e internacionales, es un mecanismo que representa varios de los principios y mecanismos actualmente implementados en ICANN, IGF y en Plan de Acción de la Sociedad de la Información en América Latina y el Caribe (ELAC), por ejemplo. Tanto el CCI, como el Grupo Iniciativa y la Mesa Colombiana, así como los ejemplos incipientes en Venezuela y Uruguay muestran una alta adhesión a los principios y prácticas asociadas al proceso de trabajo en el marco de ELAC y el LACIGF en la región, así como el IGF a nivel internacional.

Conclusiones y recomendaciones

Este trabajo examina los mecanismos nacionales de gobernanza de internet en los procesos iniciales de institucionalización. Aborda los principales desarrollos que han moldeado tanto las estrategias de los actores organizados incipientemente en torno al tema de la gobernanza de internet, en conformaciones que en algunos casos asoman como una policy network (Argentina, México, Uruguay, Venezuela) y en otras experiencias comienzan a tener visos de redes gobernanza (Colombia, Costa Rica). Claramente el "CGI.br" se encuentra en esta segunda clasificación.

Siguiendo la clasificación de Peters de la sombras de la gobernanza, entendida como la autoridad que da sentido a un arreglo determinado, el capital social de pioneros de internet en estos países consolidó mecanismos de gobernanza que inicialmente se encontraban basados en el conocimiento de los expertos. Esas configuraciones se encuentran especialmente presentes en la actualidad en los casos de México y Costa Rica, y en menor medida en Argentina, Uruguay y Venezuela. Investigar los procesos institucionales en formación para las políticas y gobernanza de internet en la región en este momento histórico es particularmente relevante, ya que desde una perspectiva institucionalista, estos comienzos luego tienden a marcar mecanismos que refuerzan las opciones iniciales. Como se puede ver con la introducción de internet en estos países, muchos de estos actores continúan a la fecha invo-

lucrados en los recientes mecanismos nacionales de políticas y gobernanza de internet. Es aún prematuro evaluar el legado de estas iniciativas, más allá de la organización de los foros nacionales de gobernanza de internet, que constituyen un punto visible de discusión y de formación de agendas.

El concepto de red de políticas, y su evolución a una red de gobernanza se encuentra en pugna con la idea tradicional que las políticas se definen unilateralmente por parte del Estado. Como ya fue señalado, las contribuciones de estos procesos al entorno de las políticas en esta materia resultan aún incipientes. Es también complejo de evaluar en tanto la propia internet es una tecnología difícil de regular mediante instrumentos tradicionales, y por lo tanto muchos de los avances que estos mecanismos están desarrollando son de carácter procesual e intangible. Las brechas de participación y los niveles de subsidiariedad destacados al comienzo del trabajo como relevantes para la provisión de bienes públicos globales, son aspectos que estos procesos nacionales están atendiendo, aun cuando todavía hay un déficit en la capacidad de participación y de incidencia en las agendas y en los mecanismos regionales como el LACIGF o el ELAC, así como en el IGF. Existe una mayor necesidad de atender a los asuntos domésticos, muchas veces impuestos por las agendas de los gobiernos y sus procesos regulatorios y legislativos, más que a los temas que pueden estar coyunturalmente menos visibles en la agenda o que requieran de mayores esfuerzos de seguimiento y coordinación de mediano plazo, como es el caso en las instancias regionales y globales. En esta línea, una recomendación para estos mecanismos sería avanzar en estas iniciativas en dos frentes: por un lado, enfocándose en los problemas de internet de ese país, caracterizando los temas con el valor del conocimiento específico y local y la priorización correspondiente, y por otro, desplegar una línea de seguimiento más activa a los espacios regionales y/o internacionales donde se desarrollan temas de gobernanza de internet y donde actores como la academia y la sociedad civil tengan capacidad de incidencia. Esta dimensión regional e internacional es fundamental, ya que buena parte de los asuntos relacionados con internet desde una perspectiva de gobernanza no están únicamente circunscriptos a jurisdicciones y territorios, por lo que la retroalimentación resulta esencial para enriquecer ambas experiencias.

Otra recomendación para fortalecer la relevancia de estos espacios es el desarrollo de mecanismos de trabajo más permanentes, en lugar de estar solo enfocados en la organización del IGF nacional (o su nombre equivalente), intentando que estos resultados sean públicos. Esto se debe a que el trabajo más distribuido hace más visible el trabajo y los logros que la realización de un evento anual. De todas formas, cabe señalar que muchos

de estos mecanismos se comportan como espacios de trabajo transversales, como es el caso del CCI de Costa Rica (que ni siquiera organiza un foro de gobernanza de internet en el país), el CGI de Brasil (que solo en los últimos años comenzó a organizar el foro nacional), la Mesa Colombiana o el Grupo Iniciativa. En los casos más incipientes, como el de Argentina, Uruguay o Venezuela el objetivo de estos espacios aún está centrado en consolidar procesos para la creación de un foro multisectorial.

Un elemento adicional que puede considerarse una "buena práctica" de varias de estas experiencias es el uso de herramientas de colaboración online para el desarrollo del trabajo, tanto a nivel de discusiones como de documentos y propuestas (es muy notorio en los casos de Costa Rica, México y Colombia). De esta forma, el trabajo se vuelve más transversal a la vez que se genera una "memoria institucional" para los futuros actores que vayan a sumarse.

En relación a la contribución académica en estos espacios, es interesante destacar que la misma es conceptualizada como "sociedad civil" en el IGF, y que en otros espacios con mayor presencia de ingenieros puede estar asociada a la "comunidad técnica". Sin embargo, el rol de la academia y de los académicos en estos espacios y mecanismos nacionales tiene una visibilidad mucho más clara, y puede transformarse en un actor con una identidad más definida de la que posee en otros espacios regionales e internacionales. Estas contribuciones académicas pueden vincularse con la capacidad de producir información primaria, e investigaciones y argumentos sustentados en evidencia empírica y/o cuerpo disciplinario.

Por último, la excesiva formalización con consecuencias sobre la rigidez de algunos de estos mecanismos no debería confundirse como sinónimo de un proceso nacional más consolidado. La experiencia del CGI en Brasil es la de un modelo corporativo, con reglas y pautas claras, y una trayectoria de más de 20 años de funcionamiento, y un sistema de financiamiento asociado los recursos de internet que no necesariamente debe ser replicado como modelo en otros contextos nacionales en los que aún la red de políticas en torno a la gobernanza de internet no se encuentre lo suficientemente desarrollada. Será necesario en estos casos consolidar experiencias que, aun no siendo demasiado formales, tengan continuidad en el tiempo y produzcan algunos resultados tangibles –ya sea como foros nacionales o documentos– para atraer a más actores de los distintos sectores, así como para posibilitar el desarrollo más equilibrado de políticas públicas y regulación en materia de internet.

Otras referencias

Hemmati, Minu, *Multi-stakeholder Processes for Governance and Sustainability: Beyond Deadlock and Conflict*, Londres, Earthscan Publications Ltd., 2002. Disponible en: http://bit.ly/2fCGxVU

Kenis, Patrick y Schneider, Volker, "Policy Networks and Policy Analysis: Scrutinizing a New Analytical Toolbox", en: B. Marin y R. Mayntz (eds.), *Policy Networks: Empirical Evidence and Theoretical Considerations*, Fránfort, Campus Verlag, enero de 1991. Disponible en: http://bit.ly/2ffbgru

Kooiman, Jan, "Governance. A Social-Political Perspective", en: Grote, J. y Gbikpi, B. (eds.), *Participatory Governance: Political and Societal Implications*, Opladen, Leske + Budrich, 2002, pp. 71-96.

Lucero, Everton, *Governança da internet: aspectos da formação de um regime global e oportunidades para a ação diplomática*, Brasilia, Fundação Alexandre de Gusmão, 2011.

Mariscal, Judith, Rivera, Eugenio y Naciones Unidas, *Regulación y competencia en las telecomunicaciones mexicanas,* México, D.F., Naciones Unidas, CEPAL, Unidad de Comercio Internacional e Industria, 2007.

Núñez, Mauricio Guido, *Tutela de los nombres de dominio en Internet*, 2004, disponible en: http://bit.ly/2fZy13Z

Olson, Mancur, *The logic of collective action: Public goods and the theory of groups*, Cambridge, Massachusetts, Harvard University Press, Enero 1971. Disponible en: http://bit.ly/1EG6zOe

Quarterman, Jon, *"Networks in Argentina", Matrix News*, Vol. 5, Nº 8, Texas, Matrix Information and Directory Services Inc., 1991.

Rhodes, R.A.W., "The New Governance: Governing without Government", en: *Political Studies*, Vol. 44, Nº 4, 1996, pp. 652-667.

Capítulo Dos

Ciberseguridad y derechos humanos en América Latina

Daniel Álvarez Valenzuela[1] y Francisco Vera Hott[2]

Introducción

Desde fines de la década del 2010, diversos sucesos han puesto a la ciberseguridad vertiginosamente de moda: ataques de denegación de servicio en Estonia, uso de ciberataques en Georgia, la consolidación en ciertos países de la ciberdelincuencia organizada, fugas y filtraciones masivas de información de empresas y Estados, uso de *malware* e interceptación de comunicaciones digitales por parte de gobiernos para perseguir activistas, entre muchos otros eventos. Todo ello amplificado por las revelaciones de Edward Snowden sobre las actividades de vigilancia masiva de comunicaciones llevadas a cabo por las agencias de inteligencia de países como Estados Unidos, Inglaterra, Nueva Zelandia, entre otros.

Estos sucesos vienen acompañados de una creciente sofisticación técnica en los medios utilizados, desde modalidades de hacking social como el *phishing* hasta el uso de amenazas avanzadas persistentes, con complejas aplicaciones maliciosas, algunas programadas específicamente para sustraer información

[1] Daniel Álvarez Valenzuela es abogado. Licenciado en Ciencias Jurídicas y Sociales y diplomado en Derecho Informático por la Universidad de Chile. Actualmente, cursa sus estudios de doctorado en la misma universidad. Es profesor de Privacidad y Tecnología de la Facultad de Derecho de la Universidad de Chile en sus cursos de pregrado y postgrado. Coordinador de Investigaciones del Centro de Estudios en Derecho Informático. Fundador y editor general de la *Revista Chilena de Derecho y Tecnología*. Fundador de la ONG Derechos Digitales. Su correo electrónico es dalvarez@uchile.cl

[2] Francisco Vera Hott es abogado. Licenciado en Ciencias Jurídicas y Sociales por la Universidad de Chile. Becario Fulbright y Thomas Buergenthal Scholar 2016-2017. Está realizando sus estudios de postgrado en la George Washington University. Su correo electrónico es francisco@verahott.com

estratégica de carácter militar o comercial, hasta otras que pueden cifrar ilegalmente los contenidos de un computador haciéndolos inaccesibles para su legítimo dueño, que deberá pagar a delincuentes informáticos para recuperar el acceso a su información. Todos estos sucesos tienen un elemento en común: han puesto a la ciberseguridad en el centro de las preocupaciones de múltiples actores, tanto públicos como privados, muchos de los cuales están realizando grandes esfuerzos para comprender los riesgos que supone el ciberespacio y las decisiones que deben adoptar para hacerles frente.

En el presente trabajo queremos hacer una revisión crítica de ciertos conceptos esenciales para la discusión. Y para ello, presentaremos a la ciberseguridad como un concepto en disputa, dando cuenta de las principales discusiones que hay a su respecto, y esbozando los estándares mínimos, desde una perspectiva de derechos humanos, que deberían observarse a su respecto, considerando ejemplos en el contexto latinoamericano.

I. Precisiones sobre el concepto de ciberseguridad

Desde hace un par de años, la expresión ciberseguridad ha ido ocupando cada vez más espacio en el debate público y privado, superando el ámbito de competencias específicas de los profesionales de la informática. Hoy por hoy vemos cómo la ciberseguridad ha provocado que gobiernos, organizaciones internacionales, universidades, empresas, organizaciones de la sociedad civil e incluso personas naturales, adopten –en sus respectivos ámbitos de acción– medidas que persiguen hacerse cargo de un fenómeno que aparentemente llegó para quedarse.

La diversidad de actores involucrados en la discusión sobre ciberseguridad –desde hackers, informáticos, ejecutivos del sector privado, funcionarios públicos, oficiales de seguridad y defensa, hasta periodistas y activistas de derechos humanos– da cuenta que cada cual utiliza los conceptos relativos al "ciberespacio" (normalmente anteponiendo el prefijo "ciber" a los términos a emplear) según su foco de atención e intereses propios, y no existe consenso respecto a un significado material de la expresión "ciberseguridad" ni mucho menos sobre sus alcances jurídicos, políticos e incluso –extrañamente– técnicos. Pero antes de hablar de ciberseguridad resulta ineludible revisar las ideas y conceptos que están detrás de los términos ciberespacio y seguridad que componen el nuevo ámbito que nos ocupa. Para ello, revisaremos sintéticamente ambos conceptos, incluyendo paradigmas particulares para nuestro enfoque relativos a seguridad, seguridad nacional, seguridad humana y seguridad de la información.

I.A. Ciberespacio

El concepto de ciberespacio –palabra que a su vez combina el término "cibernética" con "espacio"[3]– fue introducido por primera vez por el escritor de ciencia ficción William Gibson, en su cuento "Burning Chrome", quien luego lo utilizó extensivamente en su libro Neuromancer. En este último, se concibe al ciberespacio como un ámbito tridimensional de pura información que se mueve entre computadoras y donde las personas son generadoras y usuarias de esa información.[4]

En la actualidad, la mayoría de los conceptos de ciberespacio giran sobre la noción de un espacio, ambiente o dominio de la información, lo que puede apreciarse en la recopilación de definiciones publicada a fines del año 2014 por New America.[5] Todas ellas, con diversos matices, coinciden en definir al ciberespacio como una dimensión distinta a la física, donde se producen interacciones humanas sobre la base del intercambio de información.[6]

El ciberespacio está compuesto por tres capas claramente distinguibles. La primera capa corresponde a la infraestructura física (cables, computadores, satélites) que permite que el ciberespacio pueda operar como tal. La segunda corresponde a la infraestructura lógica (protocolos de red, programas de computación) que crean el lenguaje que permite la interacción entre máquinas y personas, y la tercera capa está compuesta por los contenidos y/o las interacciones humanas (textos, audios, videos, etcétera).[7] Cada una de las capas está sujeta a regulaciones distintas que pueden o no converger sistémicamente, lo cual complejiza el análisis del ciberespacio como un conjunto.

Internet, si bien hoy está en el centro del concepto de ciberespacio, no lo agota constituyendo más bien una de sus más importantes manifestaciones.

---

[3] Singer, Peter y Friedman, Allan, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford, Oxford University Press, 2014.

[4] Craigen, Dan, Diakun-Thibault, Nadia y Purse, Randy, "Defining Cybersecurity", Technology Innovation Management Review, Ottawa, Universidad de Carleton, 2014. Disponible en: http://bit.ly/2fzXhNF.

[5] Maurer, Tim y Morgus, Robert, "Compilation of Existing Cybersecurity and Information Security Related Definitions", New America Report, Washington DC, octubre 2014, pp. 18-24. Disponible en: http://bit.ly/2eB5ZGJ.

[6] Podemos encontrar algunos conceptos similares a ciberespacio, pero enfocados en ciertos aspectos específicos, como seguridad de la información o tecnologías de la información. Sin perjuicio de las diferencias, todos los conceptos apuntan a esta nueva realidad definida por el uso y el procesamiento de información digital.

[7] Benkler, Yochai, "From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access", *Federal Communications Law Journal*, No. 52, Washington DC, 1999.

El ciberespacio es algo más amplio que internet, es el ámbito de información digital incluso cuando no forma parte de esa red de redes,[8] que incluye también a las interacciones humanas que allí se producen y las interacciones de sistemas computacionales no conectados a internet.[9]

Con todo, los conceptos de ambiente, dominio o territorio que subyacen al término ciberespacio, le impregnan necesariamente una carga política, como un lugar donde existen disputas de poder en y sobre el ciberespacio, las que se manifiestan en la definición de términos como ciberseguridad. En ese sentido, cada concepto de ciberespacio y, muy especialmente de ciberseguridad, vienen de la mano con una agenda política determinada, como veremos más adelante.

I.B. Seguridad

La seguridad es un concepto muchísimo más antiguo y disputado, con discusiones en diversos frentes y disciplinas que se remontan, en la época contemporánea, a los fines de la Guerra Fría[10] y, ciertamente, no es posible abordarla de manera integral en este trabajo, pero nos centraremos en aquellas nociones que puedan resultar relevantes para arribar a una definición de ciberseguridad, descartando de plano concepciones estrictamente legales, como la seguridad jurídica, y aquellas de corte sicológico o intimista, que apuntan a la sensación de seguridad antes que al fenómeno político y social que acá nos interesa. No obstante lo anterior, aun cuando no nos es posible arribar a una definición unívoca de seguridad,[11] es posible identificar algunos de los paradigmas de seguridad más relevantes para la construcción de un concepto de ciberseguridad: seguridad nacional, seguridad humana, multidimensional y seguridad de la información.

El paradigma de seguridad clásico es el de "seguridad nacional", que deriva a su vez de la idea de soberanía.[12] Este concepto, cuya forma mo-

[8] Singer, Peter y Friedman, Allan, supra nota 3, p. 14.

[9] Un ejemplo de lo anterior es el caso de Stuxnet, programa malicioso que atacó una central nuclear que no estaba conectada a ninguna red computacional, lo que prueba la capacidad de que existan ataques en el ciberespacio que no involucren el uso de internet.

[10] Baldwin, David, "The concept of security", en *Review of International Studies*, Nº. 23, Cambridge, Universidad de Cambridge, 1997, p. 9.

[11] En diccionarios como el de la Real Academia Española, la seguridad se define como "la cualidad de seguro", y al ir al concepto de "seguro", se define como "la ausencia de fallas, riesgos, peligros o dudas", los que solo contribuyen a darle un marco funcional al concepto, pero no responde la pregunta sobre qué fallas, riesgos, peligros o dudas se pretende evitar o minimizar.

[12] "Sovereignty", *Stanford Encyclopedia of Philosophy*, University of Stanford, 2016.

derna viene de la mano de las obras de Hobbes y Bodin, fue consagrado en el Tratado de Westfalia de 164813, y en él dominan las ideas de integridad territorial, estabilidad política, arreglos militares y actividades económicas.

El paradigma de seguridad nacional tiene como protagonistas a los Estados y la mantención de su soberanía –como presupuesto de la vida en sociedad–. Este es el presupuesto de cualquier actividad política, por lo que el objetivo principal es la mantención del poder soberano del Estado. De esta forma, el gobierno debe proteger al Estado y a sus ciudadanos de todo tipo de crisis y amenazas usando sus diversas herramientas de generación y proyección de poder. Este paradigma fue adoptado explícitamente por varios países tras la finalización de la Segunda Guerra Mundial, frente a la amenaza nuclear y en el contexto de la Guerra Fría. Sobre la base de este paradigma se desarrolló la doctrina de la seguridad nacional (también conocida en el contexto americano como "seguridad hemisférica"[14]), la que amparándose en la figura del enemigo interno sirvió para justificar la toma violenta del poder y el surgimiento de dictaduras a lo largo de todo el mundo, especialmente en América Latina.[15] Además, fue utilizada por varias de esas dictaduras como fundamento a las gravísimas violaciones a los derechos humanos que afectaron a muchísimas personas. Con todo, el concepto de seguridad nacional desde la década de 1990 ha evolucionado para integrar nuevos paradigmas como la seguridad multidimensional y la seguridad humana.

En el contexto americano, el concepto de "seguridad multidimensional" nace a fines de la Guerra Fría, al emerger un nuevo panorama regional caracterizado por factores de inestabilidad comunes, que exceden el plano estatal y militar, y abarcan una variedad de temas entre los que se comprenden la pobreza, el terrorismo, el crimen organizado, el tráfico de armas y los desastres naturales.[16] El empleo del paradigma de seguridad multidimensional fue ratificado por la Organización de Estados Americanos (OEA) en octubre de 2003, en el marco de la Conferencia Especial sobre Seguridad, donde se adoptó la "Declaración sobre Seguridad de las Américas". De aquí nace una nueva concepción de seguridad hemisférica que incluye tanto amenazas tradicionales como emergentes, estableciendo

[13] Tratado de Westfalia.

[14] Rojas, Francisco y Soto, Daniel, "Estándares Internacionales y Seguridad Pública", en Revista de Derecho Público, Vol. 77, Santiago, Universidad de Chile, 2012. Disponible en: http://bit.ly/2eAWkA9.

[15] Instituto Interamericano de Derechos Humanos, ¿Qué es seguridad humana?, San José, Costa Rica. Disponible en: http://bit.ly/2af7dde.

[16] Rojas, Francisco y Soto, Daniel, *supra* nota 14, p. 444.

que los derechos humanos y las libertades fundamentales eran esenciales para la estabilidad, la paz y el desarrollo de los estados americanos.[17]

El paradigma de "seguridad humana", por su parte, implica un cambio de mirada al concepto de seguridad, poniendo al ser humano en el centro, y sus orígenes pueden ser trazados también hacia finales de la Segunda Guerra Mundial y la proclamación de la Declaración Universal de Derechos Humanos del año 1948.[18] Ya en el primer párrafo del preámbulo de la Declaración se indica que "la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia humana", dejando a los seres humanos, y no al Estado, en el centro de los desafíos de seguridad, y especificando que la seguridad del Estado no coincide necesariamente con la seguridad de las personas.

Un punto culmine de esta concepción lo constituye el Informe sobre desarrollo humano de 1994, del Programa de Naciones Unidas para el Desarrollo (PNUD), donde se define la seguridad humana a partir de dos aspectos principales: "En primer lugar, significa seguridad contra amenazas crónicas como el hambre, la enfermedad y la represión. Y en segundo lugar, significa protección contra alteraciones súbitas y dolorosas de la vida cotidiana, ya sea en el hogar, en el empleo o en la comunidad".[19] Así, se define a la seguridad humana como la libertad de las personas del miedo, de la necesidad o de la miseria y la libertad para vivir con dignidad.[20]

Desde un punto de vista técnico, tenemos el concepto de seguridad de la información, que puede resumirse en la preservación de la tríada de confidencialidad, integridad y disponibilidad de la información de un sistema.[21] La confidencialidad apunta a la mantención de la privacidad de los datos, y que solo puedan acceder a ella sus destinatarios. La integridad significa que el sistema y sus datos no hayan sigo alterados o eliminados sin la autorización o voluntad de su titular. La disponibilidad, en tanto, significa la

[17] Ibíd. (citando a: Declaración sobre Seguridad en las Américas, Organización de Estados Americanos, 2003).

[18] Declaración Universal de Derechos Humanos, París, 10 de diciembre de 1948.

[19] *Informe sobre desarrollo humano*, Programa de las Naciones Unidas para el Desarrollo (PNUD), Nueva York, 1994.

[20] Instituto Interamericano de Derechos Humanos, *supra* nota 15.

[21] El origen exacto de esta definición no está claro, aun cuando los conceptos operacionales que le sirven de sustento se remontan a numerosos tratados militares que provienen desde la antigüedad, como "*de bello Gallico*" (La guerra de las Galias), y en la actualidad es recogida por diversos estándares técnicos en la materia, como la familia de estándares ISO 27.000.

posibilidad de poder usar un sistema para los fines que fue diseñado.[22] Con todo, el concepto de seguridad de la información no se agota en los tres elementos reseñados. En otros contextos académicos, se habla de la tríada confidencialidad, integridad y autenticidad, mientras que en el ámbito de la gestión de la seguridad de la información, se procura distinguir como ámbitos de acción la interacción entre tecnologías, procesos y personas.

Finalmente, el desarrollo de redes informáticas de mayor complejidad, y particularmente el desarrollo y la ubicuidad de internet, han llevado a plantear la necesidad de integrar nuevas propiedades al concepto de seguridad de la información, como la resiliencia,[23] que permite a los sistemas resistir y sobreponerse a amenazas contra su seguridad en lugar de dejar de estar disponibles. Esto es consistente con un aspecto clave de la gestión de la seguridad de la información, que no se limita a la mera prevención de que se produzcan ataques o incidentes, sino que tiende a identificar y gestionar adecuadamente los riesgos asociados. Como todo especialista se apura en señalar, no existe un estado de seguridad absoluta en materia informática, sino sólo la posibilidad de minimizar y gestionar los casos en que ésta se vea comprometida.

I.C. Ciberseguridad

Tras revisar los conceptos de ciberespacio y seguridad, cabe analizar el de ciberseguridad, que combina ambos conceptos, y que representa la idea de seguridad en este nuevo ambiente. No existe una concepción ampliamente compartida sobre ciberseguridad, siendo este término aún más disputado que el de ciberespacio. A la fecha, según la investigación de New America,[24] es posible constatar la existencia de más de cuarenta y cinco conceptos distintos.

La ciberseguridad debe comprenderse como un fenómeno distinto de la seguridad de la información, toda vez que se trata de un concepto que dista de ser técnico o destinado a especialistas, que implica la interacción del ciberespacio con las diversas concepciones de seguridad, incluyendo en algunos casos la utilización del ciberespacio como medio o herramienta para generar amenazas a la seguridad nacional, la seguridad multidimensional en algunos de sus planos o, inclusive, la seguridad humana.

[22] Singer, Peter y Friedman, Allan, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford, Oxford University Press, 2014, p. 35.

[23] *Ibíd*., p. 36.

[24] Maurer, Tim y Morgus, Robert, "Compilation of Existing Cybersecurity and Information Security Related Definitions", *New America Report*, *Washington DC, 2*014, pp. 25-32.

De acuerdo con aproximaciones más modernas, el ciberespacio es uno más de los ambientes donde los Estados y otros actores organizados pueden construir y ejercer poder, por lo que el concepto de ciberseguridad puede ampliarse al punto de caracterizar esa disputa de poder en el ciberespacio. Dentro de dicha disputa, se comprende también el concepto de ciberseguridad y la forma en que los Estados luchan por imponer sus conceptos de seguridad y sistemas de valores en el ciberespacio. En palabras de la ministra de relaciones exteriores de Estonia, Marina Kaljurand, lo "ciber" no es una tecnología, es una noción política anclada en la convergencia de diversas tecnologías, donde el ciberespacio opera como escenario social, mercado financiero, y campo de batalla político.[25]

I.C.I. Importancia de un enfoque de gestión de riesgos y falta de un concepto compartido

Dado que es imposible prevenir del todo la ocurrencia de ciberataques, entre los especialistas existe un alto grado de consenso respecto a la importancia del enfoque de gestión y minimización de riesgos. En ese sentido, es esencial la inclusión de este enfoque en el concepto de ciberseguridad, puesto que implica una aproximación racional y proporcionada al tema, y promueve el uso de herramientas técnicas apropiadas para gestionar los riesgos dentro del ciberespacio. Además, considerar la gestión de riesgos y, con ello, la constante posibilidad de sufrir ataques o incidentes informáticos, incorpora una mirada no sólo de prevención de la ocurrencia de incidentes, sino también de la capacidad "resiliencia" o recuperación frente a éstos. Por otra parte, omitir el elemento de gestión de riesgos (o análogos a este) en una definición de ciberseguridad, allana el camino a la adopción de políticas públicas o medidas poco idóneas o desproporcionadas.

II. Temas de ciberseguridad relevantes a nivel internacional

Las nociones y conceptos de ciberseguridad se manifiestan y adquieren importancia en varios ámbitos de acción, por ejemplo, respecto a las normas de comportamiento de los Estados dentro del ciberespacio, la regulación internacional de internet, los mecanismos para enfrentar la delincuencia en el ciberespacio, y el rol que juega la vigilancia dentro de este ambiente. Nos referiremos a cada uno de estos ámbitos por separado.

[25] The International Institute for Strategic Studies (IISS), "Evolution of the Cyber Domain: The Implications for National and Global Security", 2015, p. 15-16.

II.A. Normas de conducta entre Estados y la militarización del ciberespacio

Para los Estados, el ciberespacio se ha convertido en un ambiente a través del cual es posible conducir sus relaciones económicas, diplomáticas y militares. Esta circunstancia ha abierto varios interrogantes respecto a la existencia y aplicación de normas de conducta para los actores estatales en el ciberespacio, especialmente en aquellos casos donde los conflictos que involucran a Estados y a otros actores internacionales se trasladan a este ambiente. En particular, los conflictos en el ciberespacio (también denominados "ciberconflictos")[26] están generando importantes discusiones respecto de la aplicación e interpretación del derecho internacional a estas situaciones.

En principio, existe un amplio consenso respecto a que el derecho internacional rige plenamente en el ciberespacio, debido a que las conductas reguladas en los tratados internacionales no se restringen a un ambiente específico, sino que más bien hacen referencia a las conductas en sí mismas y a las consecuencias que generan. A ello se suma que algunas conductas en el ciberespacio pueden tener impacto en el mundo físico, como el programa malicioso conocido como *Stuxnet* que inutilizó las instalaciones de una central nuclear iraní, produciendo efectos análogos a los de un ataque físico o cinético.

De esta forma, los instrumentos internacionales sobre derechos humanos y conflictos armados reciben aplicación en el ciberespacio. La discusión, sin embargo, recae en su alcance: hasta dónde es posible aplicar los tratados internacionales vigentes y en qué casos no existen soluciones definidas a disposición, así como en la definición de normas de conducta mínimas por parte de los Estados en el ciberespacio, que puedan constituir un cuerpo de derecho internacional consuetudinario con miras a ser aplicado en el ciberespacio.

El esfuerzo más relevante para solucionar estas discusiones podemos encontrarlo en el denominado "Manual de Tallinn",[27] una iniciativa académica patrocinada por la OTAN, en el cual diversos expertos en derecho internacional han indagado acerca de la aplicación de diversas normas de derecho internacional al ciberespacio, con especial foco en las normas de jus ad bellum, que regulan la conducta de los Estados frente a los conflictos

[26] Puede encontrarse un desarrollo básico de este concepto en "Evolution of the Cyber Domain: The Implications for National and Global Security", The International Institute for Strategic Studies (IISS), 2015.

[27] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013. Disponible en: http://bit.ly/2eJlfDV.

armados. Si bien no nos detendremos a analizar el contenido de dicho manual –que además está en las últimas fases de actualización y publicación de una segunda versión– conviene hacer algunas aclaraciones básicas sobre el estado del arte de esta discusión, en relación con tres circunstancias: i) el espionaje en el ciberespacio; ii) el empleo de ciberataques sin consecuencias físicas, y iii) el empleo de ciberataques con consecuencias físicas.

En primer lugar, el espionaje o sustracción de secretos no está expresamente regulado en el derecho internacional, sin perjuicio de constituir una práctica común y de larga data entre Estados. Debido a lo anterior, las actividades de espionaje realizadas por agencias como la National Security Agency (NSA) de los Estados Unidos, la Government Communications Headquarters (GCHQ) del Reino Unido u otras similares, no están sancionadas y suelen abordarse por parte de los Estados afectados a través de medidas políticas o diplomáticas. Sin embargo, como veremos más adelante, cuando estas prácticas de espionaje y vigilancia son dirigidas en contra de personas, son aplicables las disposiciones de los tratados internacionales sobre derechos humanos correspondientes, en particular aquellos derechos vinculados con la privacidad y la libertad de expresión.

Un caso que merece particular atención es el de la vigilancia masiva de comunicaciones y actividades en internet. Las revelaciones del analista de inteligencia de Estados Unidos, Edward Snowden, que salieron a la luz a partir de junio de 2013, expusieron una serie de operaciones llevadas adelante por la NSA y sus aliados en el marco de la comunidad de inteligencia conocida como five eyes.[28] La gravedad de las revelaciones de Snowden radica en el alcance masivo de las operaciones de vigilancia expuestas, incluyendo el registro masivo de datos sobre llamadas telefónicas al interior de Estados Unidos, el acceso secreto y sin contrapesos a los datos de usuarios de diversas redes sociales como Google, Yahoo o Facebook, o la capacidad de interceptar y almacenar el tráfico de internet de países completos, entre otras.

En segundo lugar, el empleo de ciberataques sin consecuencias físicas, como los sufridos por Estonia durante el año 2007, que consistieron en ataques distribuidos de denegación de servicio (DDoS) que afectaron las redes del sector financiero y gubernamental de dicho país, constituye uno de los problemas de más difícil solución en el derecho internacional, puesto que éste regula principalmente las hipótesis de conflicto armado, caracterizado

[28] Es posible encontrar un detallado archivo de las revelaciones de Edward Snowden en el sitio web del periódico inglés The Guardian denominado "The NSA files", disponible en: http://bit.ly/2cmqvxE.

por la destrucción de instalaciones físicas o pérdida de vidas humanas, lo que en estos casos no resulta tan fácil acreditar.

Considerando que las reglas de derecho internacional no son suficientes, diversas iniciativas (que incluyen, entre otras, el "Manual de Tallinn") adoptadas en órganos internacionales como la Organización para la Seguridad y la Cooperación en Europa (OSCE), la OEA, el Consejo de Defensa Suramericano de UNASUR, o los informes de los grupos de expertos de Naciones Unidas, apuntan a la construcción de normas básicas de conducta por parte de los Estados en el ciberespacio, que van desde publicar sus puntos de contacto y definiciones y la prohibición de atacar infraestructuras críticas de cada país, hasta la imposición de deberes de asistencia en caso de ataques y prohibición de atacar a través de intermediarios o *proxies*.

En tercer lugar, los casos de ciberataques con consecuencias físicas pueden ser vinculados al concepto de autodefensa y de ataque armado en los términos del artículo 51 de la Carta de las Naciones Unidas.[29] Sin embargo, no se han registrado hasta la fecha ciberataques que puedan equivaler a ataques armados con consecuencias graves para la infraestructura de un país o que cobren vidas humanas. Estos últimos serían los únicos casos donde cabría aplicar con propiedad el concepto de ciberguerra.

No obstante, desde una óptica de derecho internacional, y debido a las dificultades de encuadrar un ataque cibernético como un ataque armado, concordamos con lo propuesto por el profesor Thomas Rid,[30] quien señala que para estar frente a una guerra deberíamos estar frente a un acto político instrumental de fuerza conducido a través de herramientas digitales (código informático malicioso), que sea potencialmente letal, lo que no se condice con ningún conflicto verificado en el ciberespacio hasta el momento, y que aparentemente no se producirá.

II.B. Gobernanza de internet y ciberseguridad

Si bien internet, como ya señalamos, no equivale al ciberespacio, es hoy en día su manifestación más evidente, dado que su regulación internacional configura un interesante sistema en el que interactúan Estados, organismos internacionales, organizaciones técnicas, y otras partes interesadas como empresas del sector privado, académicos y sociedad civil, que se relacionan en un com-

[29] Carta de las Naciones Unidas, San Francisco, Organización de las Naciones Unidas, 1945.

[30] Rid, Thomas, "Cyber War will not take place", en *Journal of Strategic Studies*, vol. 35, no 1, 2012.

plejo entramado de foros y espacios técnicos y políticos -con diversa capacidad vinculante-, que se agrupan bajo la denominación de gobernanza de internet.

Este sistema de gobernanza plantea un gran desafío para la adopción de decisiones relativas a ciberseguridad. Muchas de sus discusiones han tomado lugar en foros donde tradicionalmente se discuten temas de seguridad, bajo el paradigma del multilateralismo entre Estados, mientras que las discusiones en materia de gobernanza de internet también consideran la participación activa y deliberante de otros actores no estatales, en lo que se denomina el paradigma de múltiples partes interesadas o *multistakeholder*. La experiencia comparada señala la necesidad de un trabajo conjunto entre Estados, sector privado, academia y sociedad civil. En ese contexto, el paradigma *multistakeholder* aparece no sólo como una alternativa, sino como una necesidad, dado que la mayor parte de la infraestructura de internet (y con ello, de parte del ciberespacio) se encuentra en manos privadas o es administrada por organizaciones de carácter técnico de carácter privado.

De esta forma, la relación entre gobernanza de internet y ciberseguridad presenta múltiples e interesantes desafíos. Por una parte, integrar los espacios de discusión de seguridad y de gobernanza de internet, con el objeto de abordar el fenómeno de la ciberseguridad desde una perspectiva amplia, que considere diversos aspectos técnicos y normativos de internet en su seno. Por otra parte, asegurarse que dentro de los espacios de discusión de ciberseguridad se incorporen principios de gobernanza *multistakeholder*, que permitan un debate amplio e informado, donde se consideren las posiciones de las distintas partes involucradas.

II.C. Cibercrimen y ciberseguridad

Uno de los problemas de ciberseguridad con más impacto directo en las personas es el de la ciberdelincuencia. Sin embargo, tal como en el caso de la ciberseguridad y ciberguerra, el concepto de ciberdelito es también objeto de precisiones y debates.

En principio, existen varios delitos que están relacionados con el uso de tecnologías digitales, desde conductas que atentan contra el ciberespacio como los accesos no autorizados a sistemas informáticos, robos de información, destrucción y sabotaje de sistemas informáticos, publicación de información sensible o no consentida, fraudes informáticos o secuestros de información o ransomware; pasando por delitos que usan el ciberespacio como medio principal de comisión, como los fraudes por internet, la producción y diseminación de pornografía infantil, o la infracción de derechos de propiedad

intelectual; hasta llegar a aquellos delitos donde el ciberespacio puede tener algún rol como el uso de medios de comunicación en un secuestro, o el envío de correos electrónicos en casos de extorsión. Respecto de las dos primeras categorías (delitos contra el ciberespacio y delitos donde el medio de comisión principal es el ciberespacio), en la Organización de las Naciones Unidas[31] se ha propuesto un concepto amplio que incluye ambas categorías, y una concepción restringida, que distingue entre delitos informáticos (o delitos cibernéticos en sentido estricto) y delitos relacionados con computadoras.

Por su parte, si empleamos un concepto amplio e indeterminado de ciberseguridad (vinculando ciberespacio y seguridad en sus distintas manifestaciones) es posible encuadrar dentro de estos conceptos prácticamente cualquier delito donde puedan intervenir medios digitales. Para efectos del presente trabajo, interesa determinar en qué medida la tipificación de ciberdelitos puede contribuir a la ciberseguridad, y para ello resultará de utilidad el empleo de la aproximación técnica a la ciberseguridad ya analizada (seguridad de la información), que la vincula a la preservación de la confidencialidad, integridad y disponibilidad de la información.

De esta forma, es posible apreciar que mientras la tipificación de delitos contra el ciberespacio (primera categoría) se encuentra estrechamente vinculada con la protección de la seguridad de la información, la tipificación de delitos relacionados con el ciberespacio (segunda y tercera categorías) no está directamente vinculada con la seguridad de la información, sino con la protección de diversos bienes jurídicos tales como el patrimonio, dignidad o libertad sexual, o bien con la posibilidad de autorizar a organismos de persecución penal la práctica de medidas forenses o de vigilancia que pueden afectar la seguridad de la información, lo que no solo tiene un impacto en materia de seguridad pública, sino también en relación con el derecho humano a la privacidad, como veremos.

Así, es posible determinar que los delitos encuadrados en la primera categoría contribuyen directamente a la ciberseguridad en un sentido técnico, mientras que las otras dos categorías tienen una relación más compleja con el concepto. Lo anterior no significa que los delitos encuadrados en la segunda y tercera categoría no tengan relevancia social (de hecho, suelen ser más graves) ni que deban adoptarse medidas a su respecto, sino que su origen y su justificación suelen exceder la esfera de la seguridad de la información.

Más allá de la vinculación entre ciberdelitos y ciberseguridad, entre los

[31] Lara, Juan Carlos, Martínez, Manuel y Viollier, Pablo, "Hacia una regulación de los delitos informáticos basada en la evidencia", en *Revista Chilena de Derecho y Tecnología*, Vol. 3, No. 1, Centro de Estudios en Derecho Informático, Santiago, Universidad de Chile, 2014, pp. 103 y ss. Disponible en: http://bit.ly/2fQ81ZD.

problemas asociados a su persecución se encuentra el carácter global del ciberespacio, en un contexto donde las leyes criminales son esencialmente territoriales. Con el fin de superar ese problema y facilitar la persecución internacional de ciberdelitos, el año 2001 fue suscrito en Budapest, Hungría, el Convenio sobre Ciberdelincuencia del Consejo de Europa[32] que recoge una serie de medidas que deben adoptarse en cada país, tanto en relación con la tipificación de delitos específicos como con la adopción de medidas de cooperación internacional. A inicios del año 2016, casi cincuenta Estados han suscrito el Convenio, siendo Panamá y República Dominicana los únicos países de América Latina y el Caribe que lo han suscrito, y en el mes de mayo de 2016 el Gobierno de Chile presentó ante el Congreso Nacional un proyecto de acuerdo para su aprobación y posterior ratificación.

III. Un concepto de ciberseguridad desde los derechos humanos

III.A. Vigencia de los derechos humanos en el ciberespacio

No hay duda acerca de la aplicación del derecho internacional al ciberespacio, aplicándose sus normas plenamente y sin distinción alguna. Esto se concluye, en primer lugar, a partir del texto de la Declaración Universal de Derechos Humanos,[33] que consagra los principios de universalidad e indivisibilidad de los derechos humanos sin ninguna clase de exclusión, tal como señalan el preámbulo y los artículos primero y segundo de la declaración. Lo anterior ha sido ratificado por varias declaraciones de la Asamblea General de Naciones Unidas, donde destacan la del 29 de junio de 2012, sobre la promoción, protección y disfrute de los derechos humanos en internet,[34] y la de 21 de enero de 2014, sobre el derecho a la privacidad en la era digital.[35]

III.B. Derechos humanos involucrados

Es posible partir señalando, sobre la base de lo indicado, que no existen derechos humanos determinados/particulares/específicos/puntuales que se

[32] Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001 en Budapest.

[33] Declaración Universal de Derechos Humanos, París, 10 de diciembre de 1948.

[34] Asamblea General de las Naciones Unidas, Resolución A/HRC/20/L.13, 29 de junio de 2012.

[35] Asamblea General de las Naciones Unidas, Resolución A/RES/68/167, 21 de enero de 2014.

protejan en el ciberespacio, sino más bien que todos ellos tienen reconocimiento y protección en este ambiente, sin excepción. Sin embargo, existen algunos derechos que tienen particular relevancia en el ciberespacio, por estar vinculados estrechamente a la información, en sus diversas miradas y manifestaciones. Estos derechos son los de privacidad[36], libertad de expresión e información,[37] complementados con los de seguridad y libertad personal[38] y no discriminación.[39]

La interacción de los derechos humanos y los diversos conceptos y tópicos sobre ciberseguridad es compleja y no siempre clara, puesto que los conceptos de ciberseguridad y derechos humanos se relacionan en diversos niveles. Por una parte, se complementan en una relación virtuosa en la medida que la ciberseguridad sea funcional a la protección de la privacidad, acceso a la información o libertad de expresión y seguridad personal entre otros derechos.

Tal es el caso del concepto técnico de seguridad de la información, donde la confidencialidad está en directa relación con los derechos a la privacidad y seguridad personales y la integridad y disponibilidad con los derechos de libertad de expresión y acceso a la información. Esa relación no es tan clara cuando la concepción de ciberseguridad habla genéricamente de gestión de riesgos para el ciberespacio, que pueden estar inspirados en conceptos de seguridad nacional o multidimensional, o en el concepto de seguridad de la información planteado por la SCO, que en nombre de la ciberseguridad puede involucrar un nivel de control de información incompatible con la libertad de expresión.

III.B.I. Concepto de ciberseguridad desde los derechos humanos

En orden a proponer un concepto de ciberseguridad desde los derechos humanos, es importante considerar algunos factores ya mencionados:

En primer lugar, los derechos humanos son universales e inalienables, con lo que ningún concepto de ciberseguridad puede implicar el desconocimiento o renuncia de alguno estos derechos.

En segundo lugar, los derechos humanos son indivisibles, por lo que

[36] Art. 12 Declaración Universal de Derechos Humanos, art. 11 Convención Americana de Derechos Humanos.

[37] Art. 19 Declaración Universal de Derechos Humanos, Art. 13 Convención Americana de Derechos Humanos.

[38] Art. 3 Declaración Universal de Derechos Humanos, Art. 7 Convención Americana de Derechos Humanos.

[39] Art. 7 Declaración Universal de Derechos Humanos, Arts. 1 y 24 Convención Americana de Derechos Humanos.

no es posible implicar que algún derecho humano deba ser considerado de manera separada o ceder ante otro derecho. En ese sentido, deben aplicarse criterios interpretativos que maximicen el ámbito de cada derecho, en lugar de pretender que un derecho ceda completamente ante otro.

Finalmente, resulta preferible considerar una relación virtuosa con los derechos humanos que una contradictoria, porque permite integrar antes conceptos y es funcional a los atributos de universalidad, indivisibilidad e inalienabilidad antes considerados.

De esta forma, y considerando aquellos casos donde existe una relación virtuosa entre derechos humanos y ciberseguridad, además de un nivel de claridad y precisión que sirve para poder discriminar en qué casos hablamos de ciberseguridad, como ya vimos en el caso de los ciberdelitos, es deseable utilizar el concepto técnico de seguridad de la información.

Con todo, esta aproximación no es novedosa, y recoge la discusión generada en el seno de la Freedom Online Coalition, coalición internacional de países que declara como su objeto principal la promoción de la libertad en internet. Dentro de esta coalición, se formó un grupo de trabajo denominado "Una internet abierta y segura", que se abocó a construir una nueva definición de ciberseguridad[40] con el objetivo de subirle el perfil a los derechos humanos para su consideración integral en la formulación de políticas públicas. Así, el grupo arribó al siguiente preámbulo y definición:

> Preámbulo: el derecho internacional de los derechos humanos y el derecho internacional humanitario aplican tanto en línea como fuera de ella. La ciberseguridad debe proteger la innovación tecnológica y el ejercicio de los derechos humanos. Definición: la ciberseguridad es la preservación –a través de políticas, tecnología y educación– de la disponibilidad, confidencialidad e integridad de la información y su infraestructura, así también como la seguridad de las personas tanto en línea como en el mundo físico.

Si bien es un concepto en general correcto, que recoge en esencia la definición técnica de seguridad de la información y añade menciones expresas a los derechos humanos, no define un enfoque de gestión de riesgos, sino conceptos técnicos similares pero no análogos, y el punto sobre innovación tecnológica no es realmente necesario para la definición ni mucho menos

[40] Donahoe, Eileen y Maurer, Tim, *"Why Do We Need a New Definition for Cybersecurity?"*, Freedom Online Coalition, 2016. Disponible en: http://bit.ly/2fXTme3.

se encuentra al mismo nivel que los derechos humanos. De hecho, al desarrollar el concepto, el grupo de trabajo no aborda el porqué de la inclusión de la innovación tecnológica, sino más bien a su objetivo final, mejorar la seguridad de las personas (a articular el contenido técnico, sobre la base de la norma ISO 27.000) y los medios a utilizar: políticas, tecnología y educación.

Además de la adición innecesaria de la innovación tecnológica como elemento a proteger, y la omisión de un enfoque de gestión de riesgos, creemos que este concepto de ciberseguridad puede evolucionar en el tiempo hacia la incorporación de elementos de seguridad humana en su seno, que apunte no solo a un concepto clásico de seguridad personal, sino a un concepto de ciberseguridad que, con base en la justicia, aporte a la libertad de las personas del miedo, de la necesidad o miseria y la libertad para vivir con dignidad. En el fondo, tomar los derechos humanos como base, y apuntar hacia el desarrollo como objetivo. De esta forma, creemos que el futuro del concepto de ciberseguridad desde un enfoque de derechos humanos no solo apunta a proteger ciertos atributos de la información funcionales a estos, sino también a asegurar que el ciberespacio sea un ambiente fértil para el desarrollo de las personas, permitiendo a la humanidad alcanzar nuevos estándares de libertad y dignidad.

IV. Ciberseguridad y derechos humanos en América Latina

América Latina es una región con varias particularidades, como el predominio de los idiomas español y portugués, sistemas de gobierno en su mayoría presidenciales, muchos países con un pasado autoritario, con dictaduras donde se empleó la doctrina de seguridad nacional, y que hoy en día poseen altísimas tasas de desigualdad económica y social. En este contexto, resulta interesante adentrarse y comparar casos donde algunas conceptualizaciones de ciberseguridad entran en tensión con los derechos humanos. En particular, interesa revisar algunos casos donde los conceptos, normativas y prácticas relacionados con ciberseguridad, por parte de los Estados de la región, importen una afectación y posible incumplimiento de obligaciones internacionales de derechos humanos.

Para ello, haremos un breve recuento de los esfuerzos que los países de América Latina han emprendido en torno al diseño de políticas públicas en torno a la ciberseguridad, para luego discutir brevemente casos de potencial afectación de derechos humanos en torno a la tipificación de delitos informáticos, empleo de malware y otros ataques informáticos contra personas por parte de Estados, e intentos legislativos de consagrar regímenes de vigilancia desproporcionada a través de medidas de retención de datos o de revelación de ubicación geográfica.

IV.A. Desarrollo de políticas y estrategias de ciberseguridad en América Latina

El análisis de políticas públicas en materia de ciberseguridad no se reduce a textos legales, sino que incluye también el análisis de otros instrumentos ordenadores como las políticas o estrategias de ciberseguridad, que no se reducen a regular ciertas conductas, sino a coordinar esfuerzos entre diversos sectores en torno a diversos objetivos estratégicos de políticas públicas.

La ciberseguridad, más allá de los debates en torno a su definición, es un fenómeno complejo, sistémico y multifactorial que involucra diferentes aspectos como la seguridad de las redes estatales, privadas, infraestructuras críticas, prevención de delitos, educación, buenas prácticas, alianzas público-privadas, relaciones internacionales y un largo etcétera. El diseño de políticas públicas comprensivas en la materia es un gran desafío para los Estados, especialmente frente a los posibles reduccionismos en que es posible caer en el marco del diseño de estas estrategias y políticas.

En América Latina, el desarrollo de estas herramientas ha sido más bien escaso. El *Informe Ciberseguridad 2016*, elaborado por la Organización de Estados Americanos y el Banco Interamericano de Desarrollo, presenta un pormenorizado reporte estandarizado sobre el estado de desarrollo de los instrumentos de política y estrategia sobre ciberseguridad de todos los países de América Latina y el Caribe, que distingue en cinco niveles de madurez (inicial, formativo, establecido, estratégico y dinámico) y utiliza la metodología del Centro Global de Capacidad sobre Seguridad Cibernética de la Universidad de Oxford. Los resultados son poco alentadores. De los 32 países analizados, 17 de ellos están en una "etapa inicial", esto es, no muestran ningún avance en el desarrollo de una estrategia o si han comenzado el proceso, lo han realizado sin consultar con partes interesadas. Otros 10 países se encuentran en un "nivel formativo", esto es, han articulado un esquema de estrategia con posibles consultas a las partes interesadas, y solo 3 países han alcanzado el "nivel establecido", que significa que ya cuentan con un instrumento sancionado, consultado con partes interesadas y existe cierto análisis de datos, riesgos y amenazas. El informe da cuenta que ningún país de la región ha alcanzado altos niveles de madurez en materia de ciberseguridad.[41]

Estas cifras son más o menos coincidentes con las reportadas por la

[41] Organización de Estados Americanos y Banco Interamericano de Desarrollo, "Ciberseguridad ¿estamos preparados en América Latina y el Caribe?", en *Informe Ciberseguridad 2016*.

Unión Internacional de Telecomunicaciones (UIT),[42] según las cuales únicamente Panamá,[43] Colombia,[44] Brasil[45] y Uruguay[46] cuentan con estrategias o políticas nacionales de ciberseguridad. Sin embargo, de la revisión de los documentos asociados, el documento de Uruguay solo es un decreto gubernamental que regula requisitos de seguridad de la información para los órganos públicos, por lo que no califica como una estrategia nacional de ciberseguridad propiamente tal.

Por su parte, en el mapa de ENISA[47] figura Panamá como el único país de América Latina que cuenta con una estrategia de ciberseguridad junto a Jamaica[48] y Trinidad y Tobago[49] por el Caribe, y aparecen en preparación estrategias en Costa Rica, Perú y Paraguay. A estos países se suma Chile, que desde el año 2015 se encuentra preparando una política nacional sobre ciberseguridad[50], y en febrero de 2016 sometió a consulta pública un borrador de su política. Paraguay, por su parte, también publicó un borrador de su política en abril de 2016[51] con el objeto de recibir comentarios de parte de la ciudadanía. También cabe tener en consideración el caso de Argentina, que cuenta con un programa de protección de infraestructuras[52] críticas y ciberseguridad, que concentra varias funciones que suelen coordinarse en otros países a través de una estrategia de ciberseguridad.

[42] Repositorio de Estrategias Nacionales de Seguridad de la Unión Internacional de Telecomunicaciones.

[43] Gobierno de Panamá, *"Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas"*, 2015, p. 35.

[44] Colombia cuenta con dos herramientas de política pública de ciberseguridad: el documento Conpes 3.701 de *"Lineamientos de política para ciberseguridad y ciberdefensa"*, y el documento Conpes 3.854 *"Política de Seguridad Digital"*.

[45] Brasil, aun cuando no cuenta con un documento de estrategia de ciberseguridad equivalente al de otros países, cuenta con una serie de herramientas que configuran un esfuerzo coordinado de planificación política en la materia, donde destaca el *Libro verde de seguridad cibernética de Brasil*, una guía de seguridad para las infraestructuras críticas de la información; una estrategia nacional de defensa y una estrategia general de tecnologías de la información que considera un eje de seguridad.

[46] República Oriental del Uruguay, CM 827, 7 de abril de 2014.

[47] European Union Agency for Network and Information Security, National Cyber Security Strategies.

[48] Gobierno de Jamaica, National Cyber Security Strategy.

[49] Gobierno de la República de Trinidad y Tobago, Comité Interministerial sobre Ciberseguridad, National Cyber Security Strategy.

[50] Comité Interministerial sobre Ciberseguridad del Gobierno de Chile, Glosario.

[51] Gobierno de Paraguay, Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICS), Plan Nacional de Ciberseguridad.

[52] Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad de la República de Argentina.

IV.B. Conceptos de ciberseguridad en la región

Las estrategias y políticas antes reseñadas, tanto en las definiciones formales que ofrecen como en el desarrollo de sus objetivos, reflejan algunas de las nociones que hemos discutido previamente en este trabajo. Por razones de espacio y diversidad, analizaremos los casos de Argentina, Brasil, Chile y Colombia, que grafican algunos de los puntos en discusión.

Entre los países individualizados en el punto anterior que cuentan con algún nivel de desarrollo de estrategias de ciberseguridad, existen algunos donde no es posible encontrar una definición formal y establecida de ciberseguridad, siendo el caso más paradigmático el de Argentina, que no cuenta con ninguna definición formal del término,[53] como concluye la Asociación de Derechos Civiles de Argentina, en una investigación dedicada precisamente a develar qué se entiende por ciberseguridad en dicho país. Lo anterior sucede a pesar de que el concepto se usa reiteradamente en decretos y otros documentos oficiales.

Otro país donde cuesta encontrar una definición precisa es Brasil, probablemente debido a que no cuenta con un instrumento central de estrategia en materia de ciberseguridad. No obstante lo anterior, es posible encontrar una interesante definición recogida en el *Libro verde de seguridad informática*: "el arte de asegurar la existencia y continuidad de la sociedad de información de una nación, garantizando y protegiendo en el espacio cibernético, los activos de información de sus infraestructuras críticas".[54] Este concepto, que cubre algunos de los aspectos analizados, es criticable al no emplear un enfoque de gestión de riesgos, ni resolver las tensiones conceptuales entre los paradigmas disponibles de seguridad.

En Chile, existe una definición de ciberseguridad, contenida en el Decreto Supremo No. 533/2015,[55] que crea un Comité Interministerial sobre Ciberseguridad, y define este último término como "aquella condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones

[53] Asociación por los Derechos Civiles (ADC), area de Privacidad, *"Descubriendo la agenda de ciberseguridad de América Latina: el caso de Argentina. Segunda entrega: marco normativo"*, Argentina, 2016, p. 11. Disponible en: http://bit.ly/2fkM68z.

[54] Presidencia de la República, Gabinete de Seguridad Institucional Secretaría Ejecutiva Departamento de Seguridad de la Información y Comunicaciones, *Livro verde segurança cibernética no Brasil*, 2010, p. 56. Traducción libre de *"Segurança Cibernética: arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas"* (Portaria 45 SECDN, 2009).

[55] Gobierno de Chile, Decreto Supremo No. 533.

que se verifican en el ciberespacio, como también el conjunto de políticas y técnicas destinadas a lograr dicha condición".

Este concepto, que va en la línea de lo que varios países han definido como ciberseguridad, resuelve aspectos básicos en torno a esta definición, especialmente en lo referido a que el objetivo es la reducción de riesgos, y no su supresión, lo que implica una mirada desde la necesidad y proporcionalidad de las medidas en juego, lo que resulta compatible con un enfoque de derechos humanos. Además de lo anterior, hace alusión a las infraestructuras físicas, lógicas e interacciones dentro del ciberespacio, dejando fuera del concepto el contenido de esas interacciones, lo que protege al ciberespacio como plataforma o espacio de expresión e intercambio de información, pero no en cuanto a la naturaleza de los contenidos que allí circulan, dejando fuera del concepto de ciberseguridad varias discusiones sobre este punto, especialmente lo relativo al control, censura o vigilancia de contenidos nocivos.

Finalmente, merece atención el caso de Colombia, que recientemente presentó una nueva iteración en su trabajo de elaboración de políticas de ciberseguridad. En el año 2011, dicho país preparó un documento (Conpes 3.701) de "Lineamientos de política para ciberseguridad y ciberdefensa", que define ciberseguridad como la "capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética".[56] Este concepto fue criticado por la indeterminación y por los riesgos a los que se alude en el mismo, que se especificaron como "amenazas o incidentes de naturaleza cibernética", pudiendo encuadrar demasiadas situaciones bajo esta denominación.

Estas críticas fueron bien acogidas en la preparación del nuevo Conpes 3.854, que plantea una política nacional de seguridad digital, y presenta una nueva definición de ciberseguridad, en los siguientes términos:

> Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio.[57]

[56] Consejo Nacional de Política Económica y Social República de Colombia, *"Lineamientos de política para ciberseguridad y ciberdefensa"*, 2011, p. 39.

[57] Consejo Nacional de Política Económica y Social República de Colombia, *"Política nacional de seguridad digital"*, 2016, p. 87.

Sin perjuicio del análisis del documento completo y su implementación, que merecen un análisis en profundidad, el concepto de ciberseguridad contenido en el Conpes 3.854, recién referido, implica un avance en la discusión regional, presentando un interesante desarrollo conceptual que cubre las herramientas y objetivos específicos de la ciberseguridad, recogiendo elementos de seguridad de la información (como la preservación de la confidencialidad, integridad y disponibilidad), sumando la autenticación y no repudio, y dejando como objeto principal de protección a los usuarios y activos de la información.

De esta forma, el concepto que presenta Colombia permite orientar de mejor manera las decisiones de política pública en materia de ciberseguridad, y además es mucho más funcional y acorde a un enfoque de derechos humanos en el ciberespacio.

IV.C. Tensión entre concepciones de ciberseguridad y derechos humanos en América Latina

Además del desarrollo conceptual del término ciberseguridad, la región también ha sido escenario de numerosos casos donde la aplicación de políticas públicas en nombre de éste entra en tensión con el derecho internacional de los derechos humanos.

También existen casos donde lo que está en cuestión no es el concepto de ciberseguridad, sino el uso de herramientas digitales para la afectación ilegítima de derechos humanos, vulnerando la seguridad de la información de las personas en el ciberespacio sin que en algunos casos exista claridad respecto de la necesidad o proporcionalidad en su aplicación.

Debido a la imposibilidad de un análisis exhaustivo de cada caso, nos referiremos a las categorías que grafican de mejor forma la tensión antes descripta: la tipificación de ciberdelitos que afectan el ejercicio de derechos humanos y el uso de herramientas de vigilancia digital que suponen una potencial vulneración al derecho humano a la privacidad.

IV.D. Tipificación de ciberdelitos y derechos humanos

En los últimos cinco años, en diversos países de América Latina, como Argentina, Brasil, Chile, Perú, Paraguay y México, se ha intentado introducir –en algunos casos con éxito– leyes donde se tipifican conductas que importan un legítimo ejercicio del derecho de libertad de expresión, como la crítica pública a las autoridades, la creación de cuentas de parodia en redes sociales, y el mero uso de determinadas herramientas informáticas, entre otras. Muchos

de estos tipos penales no están pensados desde un paradigma de protección de la confidencialidad, la integridad o la disponibilidad de la información en el ciberespacio, ni parten de un enfoque de gestión de riesgos, sino que aluden a consideraciones de diversa naturaleza, vinculadas con política criminal.

En estos casos el desafío es, en primer lugar, realizar un análisis fundado de la necesidad de tipificar ciertos delitos que tengan relación con el uso del ciberespacio, sobre la base de la evidencia, el derecho penal y las recomendaciones internacionales en la materia. En segundo lugar, y en caso de que sea necesaria la tipificación de alguno de estos delitos, emplear un enfoque de derechos humanos para que su afectación se dé en un marco de estricta necesidad y proporcionalidad. Otro desafío relevante es evitar el uso del concepto de ciberseguridad como un comodín que pueda justificar cualquier nuevo tipo penal en relación con el ciberespacio, sino que distinguir el bien jurídico protegido en cada caso, y argumentar en consecuencia.

IV.E. Uso de herramientas de vigilancia digital y derechos humanos

Dentro de las discusiones sobre ciberseguridad, comúnmente se habla de la vigilancia del ciberespacio[58] como una de sus manifestaciones, en circunstancias que la relación es más bien inversa, al afectarse negativamente la confidencialidad de la información mediante estas prácticas cuando se conducen de manera innecesaria y desproporcionada en contra de los usuarios. Junto con lo anterior, algunas prácticas de vigilancia, como la retención, recolección y/o almacenamiento masivo de datos y metadatos en el ciberespacio, afectan también el derecho humano a la privacidad o a la inviolabilidad de las comunicaciones, al constituir una injerencia arbitraria en la vida privada de las personas.

En ese contexto, algunos Estados de la región cuentan con legislaciones que obligan a los prestadores de servicios de internet a retener datos de sus usuarios, como su ubicación, las horas de conexión y direcciones IP utilizadas al navegar, mientras que otros han aparecido vinculados con sendos reportes que consignan el uso de programas informáticos maliciosos *(ma-*

[58] Varias organizaciones de la sociedad civil, como ADC Digital (en el reporte ya citado) identifican a la vigilancia digital como una de las acepciones comúnmente empleadas –y la que despierta más críticas de la sociedad civil– de ciberseguridad. Como indicamos al comienzo de este trabajo, la vigilancia en el ciberespacio, especialmente desde las revelaciones de Snowden, está más vinculada con vulnerar la ciberseguridad que con la aplicación de este concepto.

lware) con la finalidad de vigilar subrepticiamente a personas determinadas.

Respecto a las legislaciones de retención de datos, países como Chile cuentan con un régimen de retención de datos de conexión a internet por un año, a disposición de la Fiscalía de dicho país, sin que medie la necesidad de autorizaciones judiciales para acceder a estos datos. Perú[59] y México,[60] por su parte, cuentan con normas que consagran la retención de datos de ubicación de los usuarios de internet.

Sobre el uso de *malware*, en informes del Citizen Lab de la Universidad de Toronto[61] y de la ONG Derechos Digitales[62] consta que varios Estados de la región (Chile, Ecuador, Paraguay, Venezuela, México, Honduras, Colombia y Brasil) han adquirido de dos empresas (Hacking Team y Gamma Group) plataformas capaces de infiltrar en dispositivos digitales de personas determinadas programas maliciosos que sirven para vigilar la actividad de dichos dispositivos y la información ambiental que estos puedan captar.

La falta de transparencia en la adquisición de estas herramientas –que se han conocido principalmente por investigaciones técnicas y filtraciones–, sumado a la poca claridad de si su utilización es consistente con el derecho interno de cada país y los estándares aplicables de derechos humanos, genera un gran desafío para los Estados de la región, en torno a contar con mejores estándares de transparencia para la adquisición y uso de las herramientas utilizadas para recolectar y procesar información.

Con todo, la finalidad de ambas prácticas (retención de datos y uso de *malware* de vigilancia) sirve tanto a objetivos policiales como de inteligencia, y representan un gran desafío a abordar en lo que respecta a la intersección de ciberseguridad y derechos humanos.

V. Conclusiones

La ciberseguridad es un concepto en disputa y las discusiones sobre la materia parten de diversos presupuestos técnicos y políticos, y no existe consenso internacional respecto a su contenido material. De hecho, ni siquiera hay acuerdo acerca de que el concepto en discusión sea efectivamente el de

[59] Argote, Carlos, *"Vigilancia masiva en Perú: Ley Stalker"*, Oficina Antivigilancia, 09/11/2015. Disponible en: http://bit.ly/2eJxxwW.

[60] Forbes Staff, "¿De qué va la Ley de Geolocalización?", en *Forbes*, Ciudad de México, 16/01/2014. Disponible en: http://bit.ly/2fABRhb.

[61] Archivo de artículos y reportes sobre la materia disponible en: http://bit.ly/2fwmSVc

[62] Pérez de Acha, Gisela *"Hacking Team: malware para la vigilancia en América Latina"*, ONG Derechos Digitales, Marzo 2016. Disponible en: http://bit.ly/1S0Tku6.

ciberseguridad. Solo sería posible decir, remitiéndonos a la raíz del término, que la ciberseguridad implica una clase de relación entre el ciberespacio y la seguridad, y que este último concepto también admite diversas miradas, presentando a muy grandes rasgos los paradigmas de seguridad nacional, seguridad multidimensional y seguridad humana, junto a la concepción técnica de seguridad de la información.

Teniendo lo anterior en cuenta, los debates públicos sobre ciberseguridad no deberían asumir que existe un concepto compartido sobre la materia, y mucho menos extender a la ciberseguridad un paradigma de seguridad nacional que ya raya en la obsolescencia. De esta manera, más allá de abrazar o criticar el concepto, es necesario transparentar los valores y concepciones presentes al utilizarlo, reconociendo que existen diversas miradas a su respecto y apuntando a generar un entendimiento común que reconozca dichas miradas. También es posible concluir que la ciberseguridad es un fenómeno que abarca varios dominios, que a la fecha pocos países en América Latina lo han enfrentado de manera integral.

Asimismo, la ciberseguridad –más allá de la definición que se adopte– es un fenómeno que requiere ser abordado de manera sistémica, considerando varias dimensiones como la adopción de estándares técnicos adecuados, políticas criminales efectivas, brechas culturales, y diplomacia y normas internacionales, entre otras. De esta forma, abordar la ciberseguridad de manera integral no es un problema únicamente técnico, policial, educativo o diplomático, sino que abarca todos ellos, y para poder hacerlo de manera efectiva se requiere el involucramiento de la mayor cantidad de partes interesadas, y un modelo de gestión que sea capaz de darles participación y relevancia en los procesos correspondientes.

En el marco latinoamericano, es posible apreciar cómo el discurso sobre ciberseguridad careció (y aún carece, en algunos casos) de una mirada sistémica, enfocándose más bien en problemas y discursos específicos, los que tienden a una visión reduccionista del problema. No obstante, los esfuerzos llevados adelante por países como Chile, Colombia, Jamaica y Paraguay, desde el año 2015, muestran una evolución respecto al diseño de políticas, con una visión más integradora de la ciberseguridad.

Resta aún analizar si la implementación de estas políticas es consistente con lo allí declarado, y es capaz no solo de equilibrar, sino de partir desde el respeto integral a los derechos humanos en dicho proceso.

V.A. Recomendaciones para orientar las discusiones sobre ciberseguridad hacia estándares de derechos humanos

Necesidad de apropiarse de un concepto de ciberseguridad sobre la base de derechos humanos y promover la elaboración de estrategias en ese sentido.

Tal como señalamos, no existe en la actualidad un concepto de ciberseguridad que genere un amplio consenso en la comunidad internacional. Ese dato representa grandes oportunidades para promover un concepto sobre ciberseguridad que incorpore en su seno una visión de derechos humanos.

En ese sentido, existen interesantes propuestas como la efectuada por la Freedom Online Coalition, que pueden servir como un interesante punto de partida, al declarar expresamente la aplicación de los derechos humanos en el ciberespacio, y al restringir los elementos de seguridad a una concepción técnica de la seguridad de la información.

Sin embargo, es posible ir más allá en la generación de un concepto de ciberseguridad que promueva a los derechos humanos mediante el empleo de paradigmas como el de la seguridad humana, que no limitan la concepción de seguridad a la estabilidad nacional o internacional, dimensiones de seguridad pública, ni a la preservación de ciertos atributos de la información.

La aplicación del paradigma de seguridad humana a la ciberseguridad presenta la oportunidad de incorporar al debate elementos de justicia social que en el contexto planteado se traducen en una agenda activa de no discriminación, acceso, desarrollo económico y autodeterminación, como manifestación de la libertad de las personas del miedo, de la necesidad o miseria y la libertad para vivir con dignidad.[63]

En ese sentido, la recomendación específica es que junto con generar conceptos de ciberseguridad que consideren un paradigma de gestión de riesgos y protección de plataformas e infraestructuras, como ya señalamos, se puedan incorporar elementos de seguridad humana que pongan énfasis en las posibilidades de desarrollo que presenta el ciberespacio y la necesidad de ampliar el alcance y confianza en este ambiente, añadiendo una faz positiva a un problema que suele enfrentarse de manera más bien reactiva.

Con todo, es imposible brindar una propuesta específica y detallada de cómo debería definirse a la ciberseguridad, ya que esta decisión dependerá del contexto político y social en que se quiera introducir esta definición, y

[63] Instituto Interamericano de Derechos Humanos, *supra* nota 15.

de los intereses particulares de quien la proponga. Sí es aconsejable buscar posturas que permitan la convergencia de las distintas miradas que pueda tener este fenómeno y, en particular para la sociedad civil, integrar la mirada del ejercicio de derechos humanos en el ciberespacio con la que propicia mayores niveles de acceso y menores barreras de entrada a este ambiente.

Implementar soluciones de gobernanza en ciberseguridad que consideren roles activos para las múltiples partes interesadas.

Finalmente, como ya señalamos a propósito de la relación de la gobernanza de internet y la ciberseguridad, existe un gran desafío en cuanto a la necesidad de integrar los espacios donde actualmente se discuten temas de seguridad con aquellos ya consolidados de gobernanza de internet. En este punto, es importante acercar a los gobiernos de la región –muchas veces más experimentados en discusiones de seguridad que en gobernanza de internet– a las lecciones y experiencias aprendidas en los espacios de gobernanza de internet, invitándolos a integrarse en esas discusiones.

Para actores no gubernamentales, un gran desafío es entender los espacios donde tradicionalmente se discuten temas de seguridad, identificando los discursos predominantes y desarrollando estrategias para integrarse en estos espacios de manera constructiva.

Más allá de la relación entre espacios de seguridad y de gobernanza de internet, es importante superar la concepción rígida sobre los roles que deben adoptar los diversos actores en el debate público, e implementar modelos de gobernanza innovadores para la ciberseguridad, que consideren el paradigma multistakeholder y pueda sumar las capacidades de todos sus miembros en orden a contar con un ciberespacio seguro.

Lo anterior es particularmente cierto respecto a la sociedad civil, actores que no son siempre considerados en estos debates, y que son de especial importancia para el desarrollo participativo de modelos de ciberseguridad sobre la base de un respeto irrestricto a los derechos humanos.

Capítulo Tres

Neutralidad de la red, *zero-rating* y el Marco Civil de Internet

Luca Belli[1]

Introducción

Durante la última década, la neutralidad de la red (NR) ha sido una temática profundamente analizada en todo el mundo, que involucra a múltiples actores tanto en Brasil como en diversos foros internacionales. La neutralidad de la red se define como el principio de no discriminación cuyo objetivo es preservar la apertura de internet y facilitar al usuario final el pleno goce de sus derechos, razón por la cual ha sido consagrada en diversos instrumentos regulatorios nacionales e internacionales. En Brasil, la NR se encuentra explícitamente protegida por la Ley 12.965 (2014) más conocida como el Marco Civil de Internet (MCI) *(Marco Civil da Internet)*, es decir, el Marco de los Derechos Civiles para el uso de internet, que con-

[1] Luca Belli es Doctor en filosofía e investigador titular del Centro de Tecnología y Sociedad (CTS) de la Fundación Getulio Vargas, Facultad de Derecho, Río de Janeiro, donde dirige el proyecto "Gobernanza de Internet @ FGV". Luca también es investigador asociado del Centro de Derecho Público Comparado de la Universidad de París II. Antes de unirse al CTS, Luca trabajó para la Unidad de Gobernanza de Internet en el Consejo de Europa, ejerció como experto en Neutralidad de la Red para el Consejo de Europa, también como consultor para la Internet Society y como investigador de doctorado en la Universidad Panthéon Assas (París II). Es también el fundador y copresidente de la Coalición Dinámica sobre Neutralidad de la Red del Foro de Gobernanza de Internet de las Naciones Unidas, así como el cofundador y copresidente de la Coalición Dinámica sobre la Responsabilidad de la Plataforma y la Coalición Dinámica sobre la Conectividad Comunitaria. El trabajo de Luca sobre neutralidad de la red ha sido utilizado, entre otros, por el Consejo de Europa con el fin de elaborar una Recomendación del Comité de Ministros sobre la Neutralidad de la Red. Es autor de *De la gobernanza a la regulación de la internet (De la gouvernance à la régulation de l'internet)*, editado por Berger-Levrault, París, y coautor del *Compendio sobre neutralidad en la red (Net Neutrality Compendium)*, editado por Springer. Luca es también coeditor de Medialaws.eu. El presente artículo es una versión traducida al español del original en inglés.

siste en una ley federal que establece los principios y reglas fundamentales que regulan el uso de internet en Brasil. La evolución del debate sobre la NR influyó fuertemente en la elaboración del MCI y del decreto presidencial que estableció algunas disposiciones del MCI. Cabe destacar que las consultas públicas que llevaron a la elaboración del decreto revelaron que el *zero-rating* (ZR, tasa cero o datos de tráfico gratuitos) y su compatibilidad con la NR fue uno de los temas que más se debatieron. El *zero-rating* es la práctica de patrocinar el acceso a determinadas aplicaciones que no repercuten en la capacidad mensual de datos del usuario. Entre el 2014 y el 2016, el análisis de dichas prácticas ha estado fuertemente presente en casi todos los debates sobre neutralidad de la red. El propósito del presente artículo es contextualizar la neutralidad de la red (NR) y el *zero-rating* (ZR) a fin de explicar el reciente desarrollo de políticas y regulaciones en Brasil e impartir lecciones que pueden resultar útiles en otros contextos.

En primer lugar, el artículo examina los fundamentos de la neutralidad de la red, brinda una reseña de los debates realizados sobre la temática en todo el mundo y destaca el rol fundamental del principio de NR para permitir el pleno goce de los derechos fundamentales de los usuarios de internet (apartado I). Después de analizar el concepto de NR en términos generales, se analizarán brevemente las prácticas de *zero-rating*, al destacar la existencia de diversos modelos de ZR y revisar en detalle su compatibilidad o incompatibilidad con la NR (apartado II). En especial, se hará referencia al gran número de esquemas de ZR que apuntan a crear nuevos consumidores de servicios predefinidos en lugar de nuevos usuarios de internet, lo que determina previamente el modo en el que las personas pueden utilizar internet y limita el potencial de los usuarios finales de crear una innovación disruptiva. Dicho escenario brinda una nueva definición *de facto* de los usuarios de internet como meros consumidores en lugar de preservar su peculiar característica de "prosumidores", es decir, consumidores y a la vez productores de información, ideas e innovación.

En consecuencia, el análisis gira en torno al Marco Civil de Internet (MCI) y su función clave como principio-ley que promueve los derechos humanos, o sea, el pleno ejercicio de la ciudadanía y el acceso universal e innovación, destacando que el mismo considera a la neutralidad de la red como uno de los principios fundamentales que permite el logro de dichos objetivos, al tiempo que orienta la disciplina y el uso de internet en Brasil (apartado III). El caso de Brasil no solo representa un ejemplo de inclusión de la neutralidad de la red junto a los valores constitucionales, como la protección de los derechos humanos y la promoción de la innovación, sino que también resulta muy útil en términos prácticos para explicar que las ofertas de ZR tienden a reducir en gran medida

la apertura de internet, ya que restringen *de facto* el uso de internet de los individuos a un número limitado de aplicaciones patrocinadas. En este sentido, la combinación de una menor capacidad de datos y servicios patrocinados podría limitar potencialmente el uso general que posee internet, transformándola en una red de propósito predefinido y fomentando así la escasez artificial. De hecho, el patrocinio de determinadas aplicaciones solo cobra sentido al combinarlo con una capacidad limitada de datos, lo que representa un incentivo para que los operadores mantengan el límite de datos mensual lo más bajo posible, en lugar de promover el uso de una internet abierta. Por último, elaboraré algunas sugerencias acerca de las políticas que podrían evitar este fenómeno, a saber: la promoción de "redes comunitarias" que puedan expandir considerablemente el acceso a internet y la construcción de infraestructuras desde los extremos, que empoderarían a los individuos que, al mismo tiempo, generarían un avance positivo entre las comunidades anteriormente desconectadas.

I. El debate de la neutralidad de la red

La proliferación de los debates sobre la neutralidad de la red ha llevado a varios actores a asumir una postura al respecto, estimulando la generación de políticas de NR nacionales e internacionales.[2] Si bien se han propuesto diversos matices de la NR, la mayoría de los actores concuerda en la esencia de la misma y la define como "el principio según el cual todo el tráfico de internet debe recibir el mismo trato, sin discriminación, restricción o interferencia, independientemente de su emisor, receptor, tipo, contenido, dispositivo, servicio o aplicación".[3] Sin embargo, existe un gran debate acerca de la implementación concreta de dicho principio, y el análisis sobre la neutralidad de la red ha llegado a niveles nacionales e internacionales, generando controversias y presiones en relación con qué debería considerarse una gestión "razonable" del tráfico y la necesidad (o no) de regular la gestión del tráfico de internet.

Las controversias sobre la NR se concentran en el grado de libertad que deben tener los operadores de redes para implementar las técnicas de gestión de tráfico de internet (GTI), que puedan "discriminar" contenido, aplicaciones y servicios específicos que transiten sus redes electrónicas. Aunque puede pa-

[2] Belli, Luca and Foditsch, Nathalia "Network Neutrality: An Empirical Approach to Legal Interoperability" en Belli, L. and De Filippi, P. (eds), *Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet*, Parte III, Springer International Publishing, 6 de noviembre de 2015.

[3] Internet Governance Forum (IGF), "Policy Statement on Network Neutrality", resultados del XV Foro de Naciones Unidas sobre Gobernanza de Internet, noviembre, 2015, § 1.

recer un problema puramente técnico, conlleva enormes implicancias sociales, jurídicas y económicas. En realidad, la implementación de un tratamiento diferenciado mediante varias técnicas de GTI podría limitar excesivamente la libertad de expresión o competencia de los usuarios, cuando dichas medidas no sean necesarias y proporcionadas para el cumplimiento de un objetivo legítimo.[4]

En rigor de verdad, el debate sobre la neutralidad de la red cobró especial relevancia, ya que las técnicas de GTI pueden no solo utilizarse para un propósito legítimo, sino también para perjudicar los servicios de la competencia, bloqueándolos o degradándolos indebidamente, o para favorecer a socios comerciales a través de la priorización[5]. Dichas limitaciones indebidas son posibles ante la ausencia de políticas de neutralidad de la red, y han quedado demostradas en una variedad de contextos nacionales como en Estados Unidos,[6] Chile[7] o la UE,[8] impulsando a la creación de marcos para la neutralidad de la red.

Es importante mencionar que la GTI juega un papel fundamental para garantizar el correcto funcionamiento de las redes electrónicas, por ejemplo, al preservar la seguridad e integridad de las redes. Sin embargo, es posible que los operadores hagan un mal uso de las técnicas de GTI para favorecer o perjudicar servicios específicos, basados en consideraciones meramente comerciales. De hecho, la evolución tecnológica de los últimos quince años ha permitido a los operadores emplear técnicas de GTI que apuntan o se dirigen a

[4] Belli, Luca y Van Bergen, M., "Protecting Human Rights through Network Neutrality: Furthering Internet Users' Interest, Modernising Human Rights and Safeguarding the Open Internet", Consejo de Europa, CDMSI, Estrasburgo, Diciembre 2013, Misc. 19, disponible en: http://bit.ly/2fMPiKB; Federal Communications Commission (FCC), "Report and Order on Remand, Declaratory Ruling, and Order on the Matter of Protecting and Promoting the Open Internet". GN Docket No. 14-28. 2015; Belli y De Filippi, *supra* nota 2; y Consejo de Europa (CoE), Recomendación CM/Rec 1 del Comité de Ministros a los Estados Miembros sobre la Protección y Promoción del Derecho a la Libertad de Expresión y del Derecho a la Intimidad Respecto de la Neutralidad de la Red, enero, 2016, disponible en: http://bit.ly/2f8FlWS

[5] Body of European Regulators for Electronic Communications (BEREC), "A View of Traffic Management and other Practices Resulting in Restrictions to the Open Internet in Europe", en: *Findings from BEREC's and the European Commission's Joint Investigation*, BoR (12) 30, 29 de mayo de 2012; y FCC, *supra* nota 4.

[6] Federal Communications Commission (FCC), *Madison River Communications, LLC and affiliated companies*, Acct. Nº FRN: 0004334082, Washington D.C., 2005. Disponible en: http://bit.ly/2f8Dul1; Federal Communications Commission (FCC), "Commission Orders Comcast to End Discriminatory Network Management Practices", FCC News Media Information 202/418-0500, 1º de agosto de 2008. Disponible en: http://bit.ly/2cpWlsb.

[7] Tribunal de Defensa de la Libre Competencia (TDLC), *"Voissnet vs. CTC"*, sentencia 45, octubre de 2006.

[8] BEREC, *supra* nota 5.

aplicaciones, a servicios y a contenidos específicos, empleando las conocidas "medidas de aplicaciones específicas". Dichas medidas de aplicaciones específicas pueden discriminar servicios que estén en competencia directa con los servicios que constituyeron la base de la industria de las telecomunicaciones durante décadas, tales como voz y mensajería[1], o las aplicaciones que compiten con los socios comerciales de los operadores. Si bien la integración vertical puede resultar beneficiosa, desde una perspectiva de organización industrial, es entendible que la integración vertical[2] de los operadores de redes con los proveedores de contenidos y aplicaciones (PCA) ofrece incentivos concretos que privilegian el tráfico de los socios comerciales, mediante la priorización paga,[3] el bloqueo o la ralentización[4] de los servicios de la competencia. Por lo tanto, si bien la GTI puede ofrecer beneficios que mejoran el bienestar social tanto de los usuarios como de los operadores, también puede ser utilizada con propósitos abusivos que solo benefician a una poca cantidad de actores, es decir, de operadores y sus socios comerciales. Tal discriminación indebida puede traer consecuencias nefastas no solo para la libre competencia, sino también para la libertad de los usuarios de buscar, impartir y recibir información sin interferencia, principio que se encuentra garantizado por una serie de instrumentos legales internacionales y por la mayoría de las Constituciones Nacionales en vigencia.[5]

[1] BEREC, *supra* nota 5; Broadband Internet Technical Advisory Group (BITAG), "Port Blocking", a Broadband Internet Technical Advisory Group Technical Working Group Report, agosto de 2013. Disponible en: http://bit.ly/2fQYnVb.

[2] Cabe mencionar que el fenómeno de la integración vertical no concierne exclusivamente a los operadores de redes, dado que también se relaciona con las plataformas en línea (Comisión Europea, "Antitrust: Commission sends statement of objections to Google on comparison shopping service; opens separate formal investigation on Android", comunicado de prensa, abril de 2015. Disponible en: http://bit.ly/1FQxesN). Si bien este último tipo de integración vertical puede potencialmente perjudicar la apertura de internet y merece la atención de los reguladores, cabe mencionar que las políticas de NR no se concentran en plataformas en línea, sino más bien en los operadores que actúan en el nivel de acceso (BEREC, supra nota 5; FCC, *supra* nota 4; Belli y De Filippi, *supra* nota 2).

[3] La priorización paga hace referencia a la práctica de otorgar un trato preferencial al flujo de datos de los socios comerciales de los operadores. Los operadores presentan esta práctica como una técnica para ofrecer contenido con una calidad de servicio garantizada. La priorización paga ha sido criticada por su potencial de crear "vías rápidas de internet" y "rutas sucias", favoreciendo así a los socios comerciales y perjudicando a aquellos servicios que carecen de la capacidad financiera necesaria para pagar por prioridad.

[4] Esta práctica también se conoce como "filtrado" e incluye técnicas que limitan específicamente las velocidades de carga y descarga de determinados tipos de flujo de datos. También se la ha considerado controvertida cuando no se divulga de forma transparente y se la utiliza para discriminar el flujo de datos de los servicios competidores.

[5] Belli y De Filippi, *supra* nota 2.

Es importante mencionar que el debate sobre la NR no representa una opción binaria entre una gestión del tráfico inexistente o una gestión de tráfico gratuito. De hecho, aun los más firmes defensores del trato no discriminatorio del tráfico de internet admiten que la NR posee excepciones en relación con la gestión de tráfico razonable, mientras que incluso los más fervientes opositores de la NR admiten que los operadores no deberían involucrarse en prácticas que afecten la competencia. Si bien es cierto que la gestión de tráfico discriminatorio tiene sus beneficios cuando resulta necesaria y proporcionada para el cumplimiento de propósitos legítimos específicos,[6] y los defensores de la NR están totalmente de acuerdo, el problema es hasta qué punto pueden considerarse las prácticas de gestión de tráfico como legítimas, necesarias y proporcionadas. En este sentido, cabe mencionar que, si bien existen miradas divergentes en relación con la GTI, en general, los actores concuerdan en que la gestión de tráfico discriminatoria puede considerarse razonable siempre y cuando sea necesaria y proporcionada para el logro de algunos propósitos específicos. Particularmente, por lo general la GTI se considera razonable para fines de seguridad e integridad de la red, o para priorizar los servicios de emergencia, en caso de fuerza mayor, o cuando la GTI de protocolo específico[7] se vuelve necesaria a fin de mitigar los efectos de la congestión[8] debido a que la GTI sobre la base de múltiples protocolos

[6] BEREC, *supra* nota 5; FCC, *supra* nota 4; IGF, supra nota 3.

[7] El término "protocolo específico" describe una técnica de GTI que se dirige a una clase de aplicaciones que se ejecutan sobre un protocolo específico, tal como VoIP (voz sobre IP). A diferencia de la GTI de "aplicaciones específicas", que se dirige a una aplicación puntual, la GTI de "protocolos específicos" apunta a toda una clase de aplicaciones que explotan el mismo protocolo. El término "protocolo específico" difiere de "protocolo independiente" (protocolo agnóstico), ya que este último define una técnica de GTI que no se dirige o afecta a ninguna clase específica de aplicaciones. *Véase*, Bastian y col., "Comcast's Protocol-Agnostic Congestion Management System", RFC 6057, diciembre de 2010. Disponible en: http://bit.ly/1BKFpF4.

[8] Cabe destacar que el análisis del fenómeno de congestión no es tan simple como parece. En realidad, resulta particularmente difícil identificar de modo objetivo la verdadera causa de la congestión de la red. Tal como lo expresó Frieden: "La verdadera causa de la congestión (…) permanece esquiva. Los creadores y distribuidores de contenido especulan si los PSI han causado la congestión deliberadamente, al negarse a optimizar la capacidad de la red, o al asignar una capacidad disponible que genera la probable congestión del tráfico de determinados tipos y fuentes de contenido. Los PSI niegan este escenario y señalan circunstancias menos perversas como el clima, las vacaciones en el hogar y la decisión de los distribuidores de contenido, como Netflix, de emitir episodios para toda la temporada". *Véase* Frieden, Rob, "Net Bias and the Treatment of 'Mission-Critical' Bits", Paper Conferencia TPRC, 24 de marzo de 2014. Disponible en: http://bit.ly/2eXhbRE.

no resulta operativa[9]. Además, el uso de redes de entrega de contenido[10] (CDN, según su sigla en inglés), generalmente, se considera compatible con la NR, ya que dichas redes mejoran el rendimiento y descomprimen la congestión al agregar capacidad a las redes electrónicas, en lugar de degradar otras comunicaciones que se transmitan por los mismos enrutadores[11].

Además de utilizarse para administrar el fenómeno de congestión, las acciones de GTI también pueden ser útiles para lidiar con el uso malicioso de internet, como el *spam*, los ataques cibernéticos y el contenido y servicios ilegales. Sin embargo, tal como se mencionó anteriormente, si bien varios operadores de redes adquirieron las capacidades para manejar el tráfico de internet de modo más preciso y eficiente, por ejemplo, filtrando el *spam* o priorizando las aplicaciones sensibles a la latencia en caso de congestión, también adquirieron incentivos concretos para discriminar recursos específicos por motivos expresamente comerciales. Las técnicas de GTI pueden emplearse para garantizar el correcto funcionamiento de internet, pero también para favorecer o perjudicar paquetes de datos específicos, al tener la capacidad de distorsionar el mercado y alterar la libertad de los usuarios para buscar, impartir y recibir información sin interferencia, ante el total desconocimiento de los usuarios finales. En este sentido, varias empresas de internet han expresado que los operadores de redes "se ven motivados a discriminar y bloquear el tráfico de internet, tienen las herramientas para llevarlo a cabo y la capacidad para ocultar sus acciones, echando culpas sobre otros actores".[12]

[9] Cuando se les pidió a los distintos actores que asistieron a la IGF 2015 que expresaran su opinión sobre la caracterización de una gestión de tráfico razonable, el 84% dio una evaluación favorable o muy favorable. *Véase* Secretaría de IGF, "Idea Rating Sheet. Net Neutrality", Survey 645723, 2016. Disponible en: http://bit.ly/2f8Z3lh. Se pueden encontrar excepciones similares al tratamiento no discriminatorio en la mayoría de los marcos de neutralidad de la red.

[10] Las CDN son sistemas de red que actúan como intermediarios entre la fuente de un proveedor de aplicaciones y el operador, con el objetivo de acelerar la transmisión de los datos. See Pallis, George y Vakali, Athena, "Insight and Perspectives for Content Delivery Networks", Communications of the ACM, Vol 49, Nº 1, enero 2006, disponible en: http://bit.ly/2fNh5us. Esto se logra con el *hosting* local de las copias de datos seleccionados (*mirroring*), y ante la solicitud del usuario final, la CDN intercepta la solicitud y envía los datos desde el punto de hosteo local en lugar de enviarlos desde la fuente remota. Así, las CDN mejoran el rendimiento acortando la distancia total que deben recorrer los paquetes de datos hasta llegar a destino.

[11] BEREC, *supra* nota 5; FCC, *supra* nota 4.

[12] Internet Association, "Comments of the Internet Association in response to the Federal Communications Commission's ("Commission" or "FCC"), May 15, 2014". Disponible en: http://bit.ly/1qYaLAF.

Por lo tanto, la GTI discriminatoria puede utilizarse para fines anticompetitivos, pero también puede socavar la libertad fundamental de expresión de los usuarios. Según la Ley Internacional sobre los Derechos Humanos, los Estados poseen la obligación negativa de no interferir en el derecho de las personas de buscar, impartir y recibir información e ideas libremente, y también poseen la obligación positiva de proteger a las personas de los efectos adversos que pudieran producir las empresas privadas u otros individuos en sus libertades[13]. En este sentido, la jurisprudencia de la Corte Interamericana de Derechos Humanos (Corte IDH) y el Tribunal Europeo de Derechos Humanos (TEDH) es indiscutible en relación con la importancia del tratamiento no discriminatorio de la información y las ideas. Por otro lado, la Corte IDH consistentemente establece que "la igualdad debe regular el flujo de la información", y enfatiza que el Estado posee la obligación positiva de "extender las reglas de igualdad al mayor grado posible, para permitir la participación de las distintas informaciones en el debate público, impulsando el pluralismo informativo"[14]. Por otro lado, el TEDH ha expresado continuamente que la libertad de expresión "aplica no solo al contenido de la información, sino también al medio de diseminación, ya que cualquier restricción impuesta necesariamente interferirá con el derecho de recibir e impartir información"[15]. Dichas consideraciones también han sido continuamente reiteradas por los relatores especiales para la libertad de expresión, quienes tomaron un abordaje proactivo hacia la protección de la neutralidad de la red, enfatizando que "el tratamiento de los datos y el tráfico de internet no deben ser objeto de ningún tipo de discriminación en función de factores como dispositivos, contenido, autor, origen y/o destino del material, servicio o aplicación".[16] Por consiguiente, los gobiernos europeos han

[13] Véase Comité de Derechos Humanos, Observación General Nº 31, 29 de marzo de 2004. Disponible en: http://bit.ly/2gF4W9J ; Comisionado de Derechos Humanos del Consejo de Europa (CDHNU), informes sobre el imperio de la Ley e Internet, diciembre de 2014, § 8; Tribunal Europeo de Derechos Humanos, "López Ostra v. Spain", Sentencia Nº 16798/90, §44-58, 9 de diciembre de 1994; Tribunal Europeo de Derechos Humanos, "Khurshid Mustafa and Tarzibachi v. Sweden", Judgment Nº 23883/06, 16 de diciembre de 2008.

[14] Corte IDH, "Kimel vs. Argentina", sentencia del 2 de mayo de 2008, Fondo, reparaciones y costas, Serie C, No. 177, § 57; Corte IDH, "Fontevecchia y D'Amico vs. Argentina", sentencia del 29 de noviembre de 2011, Fondo, reparaciones y costas, Serie C No. 238, § 45.

[15] Tribunal Europeo de Derechos Humanos, (TEDH), Autronic AG v. Switzerland, 22 de mayo de 1990, sentencia Nº 12726/87. Disponible en: http://bit.ly/2h4jNf6; TEDH, Ahmet Yıldırım v. Turkey, sentencia Nº. 3111/10. Disponible en: http://bit.ly/2hoQneG.

[16] Frank LaRue (UN), Dunja Mijatović (OSCE), Catalina Botero Marino (OEA) y Faith Pansy Tlakula (CADHP), Declaración Conjunta para la Libertad de Expresión e Internet del Relator Especial, junio de 2011. Disponible en: Available at: http://bit.ly/1wnId8U.

decidido proteger de modo explícito la NR como norma de derechos humanos. De hecho, los 47 miembros del Consejo de Europa han plasmado la protección de la NR en una Recomendación del Comité de Ministros,[17] reiterando su compromiso con la neutralidad de la red, ya abiertamente expresado en la Declaración sobre la Neutralidad de la Red de 2010.[18]

Dichos compromisos surgen a partir de la observación de que el acceso no discriminatorio y la circulación de contenido, aplicaciones y servicios no solo facilita el libre intercambio de información, sino que además contribuye a reducir las barreras para ingresar al mercado de la creatividad y la innovación. En este sentido, es importante destacar que los usuarios de internet se caracterizan por ser "prosumidores", es decir, no solo son consumidores de información, sino que también son productores de innovaciones potencialmente disruptivas. Por esta razón, los actores señalan que la NR es fundamental para "preservar la apertura de internet, impulsando los derechos humanos de los usuarios de internet y promoviendo la competencia e igualdad de oportunidades, salvaguardando la colaboración de pares y diseminando los beneficios de internet a todas las personas".[19] En rigor de verdad, dentro del entorno en línea, la libertad para recibir e impartir ideas significa la libertad de acceso e intercambio de innovación, que contribuye activamente en la evolución de internet. Así, al reducir la posibilidad de los operadores de interferir con la libertad de expresión de los usuarios, el tratamiento no discriminatorio del tráfico de internet tiene el potencial de permitirles a los usuarios de internet ser desarrolladores de la innovación y ofrecer nuevas aplicaciones y servicios potencialmente disruptivos, que compitan al mismo nivel con los actores de mercado ya establecidos. En este sentido, es muy importante destacar que los usuarios de internet se consideran prosumidores y que las políticas de NR apuntan, precisamente, a facilitar dicha característica de empoderamiento. Por lo tanto, pareciera desacertado decir que las políticas de NR están en conflicto con los intereses del sector privado, según argumentan algunos opositores de la NR. Por el contrario, en general, un amplio espectro de actores comerciales respalda las políticas de NR. De hecho, los defensores del principio de NR no solo incluyen a seguidores y académicos de derechos humanos, sino también a una gran cantidad de proveedores de contenidos y aplicaciones (PCA) e

[17] CoE, *supra* nota 4.

[18] Council of Europe, Declaration of the Committee of Ministers on Network Neutrality. Adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies, 2010. Disponible en: http://bit.ly/2hAl4dx.

[19] IGF, *supra* nota 3, Preámbulo.

innovadores de empresas incipientes *(start-ups)*[20]. En general, los opositores de la NR son operadores de telecomunicaciones que poseen un importante poder de mercado y defensores de la autoregulación, tales como liberales y académicos, que argumentan que los proveedores de acceso a internet deben tener la libertad de manejar el tráfico de internet como les plazca y que la regulación de la NR podría disminuir la innovación a nivel de red e impedir la implementación de nuevos modelos comerciales, como el "pago por prioridad".[21]

Debido a la evolución de los patrones de consumo de internet,[22] en particular el crecimiento del video a demanda y los juegos en línea, los operadores han afirmado su voluntad de emplear la GTI para diferenciar el tráfico[23] y proponer esquemas de pago por prioridad, a fin de respaldar la

[20] Las empresas de internet incipientes (*start-ups*) y las ya establecidas han exigido periódicamente firmes disposiciones de NR en los diversos países en donde se han debatido las políticas de NR. Por ejemplo, en la UE, las *start-ups* establecieron la iniciativa "*start-ups for net neutrality*", también replicada en Brasil, mientras que en la India casi 700 fundadores de *start-ups* le han solicitado al primer ministro Modi que defendiera la neutralidad de la red. *Véase*, http://bit.ly/2g4EMCn.

[21] Wu, Tim y Yoo, Christofer, "Keeping Internet neutral? Tim Wu and Christofer Yoo Debate", en: *Federal Communications Law Journal*, Vol. 59. Nº 3, 2007. Disponible en: http://bit.ly/2gdkmWW.

[22] Si bien en la década de los noventa, el tráfico de internet consistía mayormente en poco ancho de banda y un lento intercambio de correo electrónico, en el año 2000, la difusión de las descargas de video y las aplicaciones entre pares generaron un mayor consumo de ancho de banda de internet, mientras que la difusión de voz sobre IP, el *streaming* de video y los juegos con múltiples jugadores generalizaron las aplicaciones sensibles a la latencia, cuya calidad comenzó a disminuir rápidamente (Ou, George, "Managing Broadband Networks: a Policymaker's Guide", The Information Technology and Innovation Foundation (ITIF), diciembre de 2008. Disponible en: http://bit.ly/1Fz48ui.

[23] La diferenciación del tráfico se basa en el uso de cualquier técnica de GTI "que clasifique y aplique un tratamiento potencialmente diferente a dos o más flujos de tráfico que se disputan recursos en una red (entiéndase por flujo a un grupo de paquetes que comparten un conjunto de propiedades en común)". BITAG, "Differentiated Treatment of Internet Traffic", 2015, disponible en: http://bit.ly/2gFtWxN. La diferenciación se basa en la explotación de múltiples clases de tráfico, que pueden tener distintos niveles de prioridad y se pueden implementar utilizando servicios diferenciados (DiffServ), servicios integrados (IntServ) o *multiprotocol label switching* (conmutación de etiquetas multiprotocolo). *Véase*, Grossman, D., "New Terminology and Clarifications for Diffserv. Request for Comments: 3260", abril de 2002. Disponible en: http://bit.ly/2hSsaKx; Baker F., Polk J. Polk and M. Dolly. M., "A Differentiated Services Code Point (DSCP) for Capacity-Admitted Traffic". Request for Comments: 5865. Disponible en: http://bit.ly/2gNRA03; y Rosen, E. y col., "Multiprotocol Label Switching Architecture" Request for Comments: 3031, 2012. Disponible en: http://bit.ly/2gPz065. A diferencia del tráfico *best-effort* (mejor esfuerzo), "el tráfico intserv o diffserv depende de los mecanismos de programación diferenciales en enrutadores congestionados, con paquetes de diferentes clases de intserv o diffserv

inversión[24] que apunta a expandir la capacidad de la red.[25] El crecimiento reciente del *streaming* de video ha requerido esfuerzos económicos para manejar la creciente demanda de tráfico,[26] presionando así a los operadores a proponer un uso extensivo de GTI para establecer distintos precios según los diferentes niveles de calidad. En este sentido, varios operadores sugirieron la necesidad de tarifas adicionales, además de las tarifas de acceso a internet ya existentes, dado que, según los esquemas de pago por prioridad, se obtendrían ingresos adicionales para invertir en la mejoría de la red. Si bien es cierto que las políticas de NR impiden a los operadores obtener ingresos adicionales de las ofertas de pago por prioridad, parece poco realista decir que más ingresos automáticamente llevarían a una mayor inversión en infraestructura, o suponer que los operadores invertirían más en infraestructura ante la ausencia de disposiciones de NR. De la misma forma, a pesar de que la ganancia neta creció 179%[27] durante el primer trimestre de 2016, Telefônica Brasil respaldó abiertamente la introducción de capacidad de datos dentro de las redes fijas en Brasil, dado que se trata de una medida necesaria para estimular la inversión.[28]

Además, al analizar la necesidad de los modelos de pago por prioridad para financiar las inversiones en redes, es importante destacar que los usuarios finales pagan a los operadores por el acceso a internet y legítimamente esperan la posibilidad de acceder y recibir el contenido, la aplicación o el servicio que ellos deseen. En este sentido, la NR se propone evitar que los operadores de red impongan un doble precio en internet, aplicando una tarifa adicional para poder acceder a contenido, aplicaciones o servicios específicos. Dicha práctica puede, en realidad, distorsionar el mercado y potencialmente impedir el acceso a contenidos y a aplicaciones que no impliquen una relación

que reciben distinto tratamiento" (Floyd, S. y Allman, M., "RFC 5290: Comments on the Usefulness of Simple Best-Effort Traffic", julio de 2008. Disponible en: http://bit.ly/2fqTt0B).

[24] Es importante mencionar que los operadores no son los únicos actores económicos que enfrentan costos e inversiones relevantes. Tal como lo mencionó Felten, no se debe considerar que los PCA se aprovechan de la infraestructura de los operadores, dado que enfrentan significativos costos recurrentes y considerables inversiones para acercar el tráfico tanto como sea posible a los usuarios finales (Felten, Benoít, "There's No Economic Imperative to Reconsider an Open Internet", 3 de abril de 2013. Disponible en: http://bit.ly/2ga5dGb.

[25] Bello, Pablo y Jung, Juan, "Net Neutrality: Reflections on the Current Debate", GCIG Paper Nº. 13, CIGI y Chatham House, mayo de 2015. Disponible en: http://bit.ly/2g9YewV.

[26] OCDE, "The Development of Fixed Broadband Networks", OECD Digital Economy Papers, No. 239, OECD Publishing, 2014.

[27] *Véase*, http://vivo.tl/2eVKTGF.

[28] *Véase*, http://bit.ly/2evlnbv.

comercial con los operadores.[29] Además, es fundamental mencionar que el atractivo de internet es una función de la posibilidad del usuario de acceder, crear y compartir contenido, aplicaciones y servicios de forma gratuita, que "son la razón de ser de internet [porque] sin correo electrónico, la web, las redes sociales, la VoIP y demás, internet sería (literalmente) inútil".[30] De este modo, basar la discriminación de contenido, aplicaciones y servicios en criterios comerciales pone en peligro los fundamentos mismos de internet, es decir, proveer una plataforma abierta de uso general para la comunicación y la innovación. Esto último resulta de gran importancia no solo debido a que la GTI no discriminatoria es esencial para permitir el intercambio de innovación a todos los usuarios, sino y principalmente porque la mayoría de los actores comerciales dentro del ecosistema de internet no son operadores de redes sino servicios web (con o sin fines de lucro), *start-ups* o empresas comunes que tienen presencia en internet. La mayoría de estos actores comerciales no tendría la capacidad financiera para pagar esquemas de priorización, o practicar *zero-rating*, como veremos en el siguiente apartado, y es por esto que se han unido a los defensores de la NR, exigiendo sólidas garantías contra la GTI discriminatoria. En este sentido, en varios países, las *start-ups* han creado coaliciones *ad hoc* exigiendo fuertes disposiciones de NR,[31] mientras que una amplia gama de empresas de internet y gigantes tecnológicos han respaldado abiertamente el concepto de que "preservar la neutralidad de internet garantiza que se mantenga como un motor para el crecimiento económico, la innovación y los valores democráticos".[32]

Muchas de las preocupaciones que surgieron en la última década en los debates sobre la neutralidad de la red, vuelven a surgir ahora en relación con el *zero-rating*. De hecho, las políticas de NR fueron adoptadas con el fin de evitar que las decisiones de los operadores pusieran en riesgo el pleno goce de los derechos de los usuarios de internet, y limiten a la vez la apertura de internet. Por esta razón, los opositores al ZR coinciden en gran medida con los defensores de NR, mientras que quienes respaldan el ZR generalmente coinciden con los opositores al NR. A continuación, se analiza brevemente la

[29] Economides, Nicholas y Tåg, Joacim, "Network Neutrality on the Internet: a Two-sided Market Analysis", en: *Information Economics and Policy Journal*, Vol. 24, Febrero de 2012, p. 91-104. Disponible en: http://bit.ly/1NCEDyX.

[30] Clark, David y Blumenthal, Marjory, "The End-to-end Argument and Application Design: the Role of Trust", en: *Federal Communications Law Journal*, Vol. 63, Nº2, Article 3, 1 de marzo de 2011, Disponible en: http://bit.ly/2fR3ODW.

[31] *Véase*, "Startups for Net Neutrality", disponible en: http://bit.ly/2fQwTx3; "Startups por uma internet livre", disponible en: http://bit.ly/2fL7Jzi.

[32] Internet Association, *supra* nota 20.

taxonomía de los modelos de *zero-rating* (ZR), según Belli,[33] estudiando la compatibilidad de ZR con los fundamentos de la NR, y planteando algunos de los costos y beneficios de dichas prácticas.

II. Modelos *zero-rating* bajo la perspectiva de neutralidad de la red

Por lo general, el término ZR describe las prácticas comerciales en las que los operadores, o un tercero, patrocinan el consumo de datos relacionado con un limitado número de aplicaciones o servicios, a los que pueden acceder los usuarios de redes móviles, sin incurrir en gastos por consumo de datos. Así, el consumo de datos de los servicios de ZR no están incluidos en la capacidad de datos de los usuarios. En ocasiones, se puede acceder a los servicios de ZR sin necesidad de un plan de datos, si bien, en general se los combina con una amplia gama de planes de datos. Dichas prácticas, generalmente se basan en la discriminación positiva de aplicaciones específicas, y han sido propuestas en países desarrollados y en vías de desarrollo, generando una nueva ola de debates sobre NR. Existen varias formas de ZR y se las puede clasificar en: (i) ZR de aplicaciones; (ii) patrocinio de aplicaciones; (iii) plataformas de ZR; y (iv) patrocinio de datos independiente de las aplicaciones.[34] El mismo proveedor puede ofrecer varias prácticas de ZR en distintos países o dentro del mismo país. A continuación, analizaremos brevemente la taxonomía de ZR, destacando la compatibilidad o incompatibilidad de los diversos tipos de ZR con los fundamentos de la neutralidad de la red (NR). Por consiguiente, se considerará el ZR desde la perspectiva brasileña.

Los esquemas de *zero-rating* apuntan a alcanzar dos objetivos que se pueden considerar fundamentales tanto desde la perspectiva de los operadores como de las grandes empresas de internet, es decir, atraer a los suscriptores de las redes de la competencia y generar nuevos clientes. Por otro lado, los esquemas de diferenciación de precios como ZR desempeñan un rol fundamental para atraer clientes y restablecer el crecimiento de las ganancias de los operadores, que tienden a disminuir cada vez más en varias regiones del mundo, en particular en Europa Occidental.[35] En este sentido, los servicios populares como los dominantes sitios de redes sociales caen dentro del esquema de *zero-rating* de los operadores con el propósito de atraer a los usuarios y aumentar la base de

[33] Belli, Luca, "Net Neutrality, Zero Rating and the Minitelisation of the Internet", en: *Journal of Cyber Policy*, Vol. 2, Londres, Routledge, 2016.

[34] *Ibíd*., profundiza el análisis de dicha taxonomía.

[35] Ovum, "Telecoms, Media and Entertainment Outlook 2015", Ovum Telecoms and Media, 2015. Disponible en: http://bit.ly/1MDDHvC.

suscriptores. Dicho escenario se observa en Brasil, en donde los operadores ofrecen esta modalidad solo para tres redes sociales dominantes: Facebook, Twitter y WhatsApp, y la popular aplicación de *streaming* de música Deezer. Por otro lado, los PCA con suficiente capacidad financiera pueden patrocinar el consumo de datos de sus servicios específicos, abonándoles a los operadores una suerte de derecho de acceso preferencial para suscriptores o nuevos suscriptores, cuyos datos personales serán luego recabados y monetizados. Este último modelo puede definirse como patrocinio de aplicaciones y difiere levemente del modelo de ZR de aplicaciones. En el modelo ZR de aplicaciones, el operador agrupa el servicio de acceso a internet y el uso ilimitado[36] de una determinada aplicación, o una determinada clase de aplicaciones, como las aplicaciones de *video streaming* o las aplicaciones de mensajería instantánea, y no recibe una comisión de patrocinio de parte de terceros. Por el contrario, en el modelo de patrocinio de aplicaciones, los costos atribuidos por los operadores al uso de una determinada aplicación se cargan al proveedor de la aplicación, que asume el rol de patrocinador. El patrocinio de aplicaciones es especialmente atractivo desde la perspectiva del operador, ya que el patrocinador es quien paga los costos, mientras que la oferta de acceso limitado a internet y servicios patrocinados probablemente capte nuevos suscriptores. Así, tanto en el esquema de ZR de aplicaciones como en el patrocinio de aplicaciones, no se le cobra al usuario el acceso a un servicio específico. La gran diferencia entre estos modelos es quién será el patrocinador que cargue con el costo establecido por el operador a fin de acceder a la aplicación.

Los esquemas de ZR antes mencionados pueden generar algunos problemas si se los considera desde la perspectiva de las políticas de NR. Tal como se mencionó anteriormente, los fundamentos de la NR consisten en evitar que los operadores discriminen aplicaciones específicas por razones comerciales, evitando así las interferencias indebidas de los operadores con la libertad de los usuarios para utilizar internet como lo deseen, lo que incluye el intercambio de innovación sobre una base de igualdad. Por el contrario, parece evidente que la decisión de patrocinar una aplicación específica u ofrecerla a través del esquema *zero-rating* se toma exclusivamente por motivos comerciales. De hecho, tanto los esquemas de ZR de aplicaciones como el patrocinio de aplicaciones se proponen dirigir la atención de los usuarios hacia un servicio percibido como gratuito, guiando así su decisión de optar por el servicio más económico en

[36] Cabe destacar que, en ocasiones, el acceso a las aplicaciones ZR no es ilimitado sino más bien limitado con una capacidad específica. En este sentido, por ejemplo, el operador TIM Brasil ofrece WhatsApp a través de *zero-rating*, pero establece una capacidad específica de 50 MB por día.

lugar del mejor servicio o el más útil. Tal como se mencionó, los operadores seleccionarán las aplicaciones que ofrecerán mediante *zero-rating* en base a que la popularidad de las mismas (que a menudo equivale al dominio del mercado) podrá atraer a los usuarios, o a la capacidad financiera del proveedor de la aplicación para subsidiar el acceso de los usuarios a esta aplicación. Si bien pueden parecer simples prácticas de mercado, es importante comprender el impacto de las mismas en el ecosistema de internet en su totalidad. La cuestión fundamental es comprender si tienen el potencial de distorsionar el ecosistema de internet al vincular el atractivo de las aplicaciones a la capacidad financiera del proveedor y no a la utilidad, eficiencia y creatividad de un determinado servicio.

Parece entendible que las prácticas antes mencionadas resulten beneficiosas al patrocinador de las aplicaciones. En este sentido, cabe destacar que cuando la revista en línea *Slate* estudió el atractivo potencial del *zero-rating*, comunicando a "los potenciales oyentes que (un determinado) podcast (de Slate) no consumiría los planes de datos de sus teléfonos inteligentes, el grupo (objetivo) fue 61% más propenso a presionar el botón *play*".[37] Sin embargo, si bien el esquema ZR puede parecer beneficioso en términos de acceso gratuito a servicios específicos, es importante aclarar que dichas prácticas pueden potencialmente convertir a internet en una red de propósito predefinido, orientando la decisión de la mayoría de los usuarios hacia el consumo de aplicaciones patrocinadas, en lugar de empoderar a los usuarios para transformarse en productores activos de la innovación.[38] En este sentido, los datos analizados por la Alianza por una Internet Asequible (A4AI, según sus siglas en inglés) en diversos países en vías de desarrollo parecen mostrar que el ZR puede distorsionar la libertad de elección, causando un fuerte impacto en el modo en que las personas deciden utilizar la internet. De hecho, si bien la mayoría de los individuos que participaron en la encuesta de la A4AI expresaron que preferirían tener una conexión total a internet por tiempo limitado o un volumen de datos limitado en lugar de acceso ilimitado a servicios específicos,[39]

[37] Knutson, Ryan, "Will Free Data Become the Next Free Shipping?", *The Wall Street Journal*, 24 de octubre de 2014, disponible en: http://on.wsj.com/1TYfgcc.

[38] Belli, *supra* nota 41.

[39] En particular, la investigación de la A4AI destaca que "un tercio de los encuestados prefiere el acceso a todos los sitios web/aplicaciones, con restricción sobre la cantidad de datos que pueden utilizarse. Una minoría de usuarios (18%) prefirió tener datos ilimitados para acceder a un número limitado de sitios (es decir, el modo en que actualmente se implementan la mayoría de los servicios de ZR). En resumen, ante la alternativa de restricción a cambio de datos 'gratuitos', la mayoría de los usuarios (82%) prefirió el acceso completo a internet, aunque dicho acceso estuviera limitado en términos de tiempo o capacidad de datos". *Véase*, Alianza por una Internet Asequible (A4AI), "Digging into the Data: Is Zero

la práctica de ZR lleva al 72% de los usuarios a dejar de utilizar los servicios de ZR. En particular, la A4AI menciona que "el 35% de todos los usuarios de *zero-rating* continúan utilizando el servicio de ZR y un plan pago [y] el 37% sigue utilizando (…) el servicio de ZR en combinación con Wi-Fi público" mientras que "el 28% de todos los usuarios de *zero-rating* ya no utiliza un plan de ZR y actualmente son clientes que pagan".[40]

La adopción del ZR en los países en desarrollo adquirió especial importancia en vistas a su propuesta de motivar la adopción de servicios en línea en áreas o países donde la penetración de internet es particularmente baja, con el fin de acortar la brecha digital existente.[41] En este sentido, algunas formas de ZR se han presentado como excepciones necesarias y proporcionadas a la NR,[42] permitiendo que los individuos sin conexión pudieran tener acceso gratuito a servicios en línea seleccionados y evitando que permanezcan completamente desconectados. Por otro lado, algunos críticos han expresado la posibilidad de emplear las prácticas de ZR para ejercer una influencia indebida y distorsionar la libertad de opinión de las personas, argumentando que el patrocinio de un restringido número de aplicaciones puede limitar la experiencia de internet de un individuo a una burbuja artificial. Dicho escenario fue concretamente descripto por Mirani, quien sugirió que el acceso a una selección limitada de aplicaciones lleva a los usuarios a creer que el servicio de ZR "es internet",[43] tal como surgió de las encuestas realizadas en diferentes países en vías de desarrollo. En este sentido, es importante mencionar que las prácticas comerciales con el potencial de afectar los patrones de consumo y la libertad

Rating Really Bringing People Online?", 2016. Disponible en: http://bit.ly/1UCwNab.

[40] *Ibíd*.

[41] La brecha digital entre los países y dentro de los mismos, responde a una serie de factores. En primer lugar, es posible que resulte difícil impulsar la conectividad debido a las barreras físicas como la falta de infraestructura, o a barreras geográficas, como cadenas montañosas o desiertos, lo que aumenta el costo de despliegue de infraestructura y lo hace poco rentable, en especial cuando la población de dichas áreas es acotada. En segundo lugar, la capacidad de las personas de conectarse puede verse seriamente condicionada al grado de alfabetismo de la población, que puede generar falta de comprensión o incluso temor a la tecnología. Por último, la pobreza de la población representa un obstáculo significativo cuando el costo del acceso a internet representa una parte sustancial del ingreso mensual promedio. Véase International Telecommunication Union (ITU), "ICT Facts and Figures", 2015, disponible en: http://bit.ly/1FOoa6p; Alianza por una Internet Asequible (A4AI), "The 2015-16 Affordability Report", 2016. Disponible en: http://bit.ly/2epYu5r.

[42] Carrillo, Arturo J., "Having Your Cake and Eating it Too? Zero-Rating, Net Neutrality and International Law", en: *Stanford Technology Law Review*, Vol. 19, Nº 3, octubre de 2016. Disponible en: http://stanford.io/2eXaHC1.

[43] Mirani, Leo, "Millions of Facebook Users Have No Idea They're Using the Internet", Quartz, 9 de febrero de 2015. Disponible en: http://bit.ly/1DbSWnK.

de opinión de una parte tan importante de usuarios deben ser cuidadosamente observadas por los reguladores, a fin de entender los potenciales costos y beneficios (sociales y económicos) que pudieran ocasionar.

Notablemente, una de las primeras cuestiones a considerar es si la preferencia de los usuarios por aplicaciones patrocinadas podría potencialmente afectar de forma negativa la pluralidad de los medios y, por consiguiente, la posibilidad de las personas de formar su opinión con libertad. Este riesgo fue evidente en la India, durante la consulta organizada por TRAI, el ente regulador nacional de telecomunicaciones, acerca de los mecanismos de discriminación de precios. Es de notar que Facebook, que fue uno de los más fervientes actores de la consulta india, favoreció el ZR, aprovechando sus propios servicios de ZR para enviar notificaciones a los usuarios, alentándolos a enviar al TRAI correos electrónicos prellenados, titulados "Respaldo *Free Basics* (es decir, el propio programa ZR de Facebook) en la India".[44] Además, las prácticas de patrocinio de aplicaciones y ZR de aplicaciones pueden considerarse como un tratamiento diferencial del tráfico de internet, ya que el tráfico específico está subsidiado a los usuarios mientras que el resto se cobra. Dicha diferenciación no es necesaria para el correcto funcionamiento de la aplicación, que se considera comúnmente como discriminación razonable, pero puede entenderse como discriminación permanente solo motivada por razones comerciales, dado que su único propósito es inclinar la decisión de los usuarios hacia las aplicaciones patrocinadas. Por último, resulta fundamental considerar que solo las aplicaciones con un valor comercial pueden ser ofrecidas en el marco del *zero-rating* por los operadores, o patrocinadas por proveedores con capacidad financiera, excluyendo así *de facto* del espectro del contenido que podría accederse de modo gratuito el acceso al contenido y los servicios no comerciales, tales como material político y educativo.

Por último, las plataformas ZR y el patrocinio de datos independiente de las aplicaciones merecen especial atención, dado que presentan distintos fundamentos y poseen distintas implicancias al compararlos con los modelos mencionados anteriormente. La plataforma ZR más conocida es la polémica iniciativa internet.org lanzada por Facebook y otras empresas de internet en 2013. El objetivo declarado por la iniciativa fue "llevar el acceso a internet y los beneficios de la conectividad a los dos tercios del mundo que no lo poseen".[45] Sin embargo, los críticos consideran que internet.org crea una

[44] Telecom Regulatory Authority of India (TRAI), "Carta de TRAI a Ankhi Das, Facebook", directora de Políticas Públicas de Facebook para India, Sur y Centro de Asia, 18 de enero de 2016. Disponible en: http://bit.ly/1WrStGc.

[45] Internet.org, *véase* http://bit.ly/23UC7rP.

internet de dos niveles para los usuarios, asignándole a Facebook el mismo "control" que los operadores desearían tener a través de la implementación de medidas de bloqueo y priorización paga. Dicho "control" les asignaría a los operadores o a Facebook, en el caso de internet.org, el poder para definir a cuáles servicios podrían accederse gratuitamente y cuáles servicios requerirían cargos adicionales a fin de orientar las elecciones del consumidor y adquirir el control en el mercado de internet. Parece importante advertir que, a pesar de que el propósito declarado de internet.org haya sido "brindar acceso a internet" a quienes no están conectados, la plataforma ha sido concebida para brindar acceso únicamente a un grupo muy limitado de aplicaciones. En rigor de verdad, como respuesta a la presión de los defensores de la neutralidad de la red y debido a la decisión de varios proveedores de contenido, entre ellos el Times Group,[46] de dejar la plataforma, Facebook la optimizó, creando el proyecto FreeBasics, que posibilita el *zero-rating* para "cualquier servicio online de poca banda ancha que cumpla con sus especificaciones técnicas".[47] A pesar de que esta modificación ha sido considerada como la intención de Facebook de crear "una plataforma abierta para que cualquiera que cumpla con los requisitos pueda participar",[48] la iniciativa original internet.org permanece intacta, es decir, solo incluye una limitada cantidad de servicios en un gran número de países en los que dicha plataforma se encuentra disponible.[49]

Cabe mencionar que en países donde las políticas públicas no logran promover la conectividad, las plataformas ZR tales como Free Basics pueden considerarse una excepción necesaria y proporcionada al principio de neutralidad de la red a fin de permitirles a las personas ejercer su derecho fundamental de libertad de expresión. Sin embargo, dichas plataformas ZR deben considerarse una solución sustentable para promover la conectividad en lugar de una solución temporaria, y deben aceptarse siempre y cuando sean abiertas a cualquier individuo que lo solicite, cumpliendo con las especificaciones técnicas necesarias para ser incluido. Como lo destacan Rossini y Moore,[50] el empleo

[46] *Véase*, Times Group, "Times Group Commits to Withdraw from Internet.org. Appeals to Fellow Publishers to Follow Suit and Support Net Neutrality", *Times Internet Corporate Blog*, 15 de abril de 2015. Disponible en: http://bit.ly/1DiNU8C.

[47] Ribeiro, John, "Facebook's Internet.org Opens Platform to Other Online Services", *Computerworld*, 4 de mayo de 2015. Disponible en: http://bit.ly/2eXwrOx.

[48] *Véase*, versión colombiana en http://bit.ly/1y9z70s y la versión keniana del proyecto en http://bit.ly/1wBONXu.

[49] *Véase*, Facebook, "Announcing the Internet.org Platform", *Facebook Newsroom*, 4 de mayo de 2015. Disponible en: http://bit.ly/1Pihrm7.

[50] Rossini y Moore, "Exploring Zero-Rating Challenges: Views From Five Countries." A Public Knowledge Working Paper., 2015.

de dichas soluciones subóptimas puede disuadir a los gobiernos de trabajar hacia soluciones óptimas dirigidas a empoderar a la comunidad no conectada mediante la provisión de conectividad plena a internet. Especialmente, para los regímenes autoritarios resulta mucho más conveniente permitir la provisión de servicios *zero-rating* previamente aprobados y fáciles de controlar que proporcionar conectividad plena a internet.[51] Este último punto es de especial importancia en vistas de que, tal como se mencionó anteriormente, la conectividad a internet les permite a los individuos no solo expresarse libremente sino también ser productores de innovación y no solo consumidores de los servicios en línea. Así, el fin último de las políticas sustentables de internet debería ser la creación de prosumidores capaces de expresarse libremente, de innovar y de competir con los pagadores establecidos, en lugar de aumentar el número de consumidores de servicios ya dominantes.

El último tipo de ZR es el patrocinio de datos independiente de las aplicaciones. En este modelo, una entidad patrocinadora subsidia una cantidad limitada de datos que el operador dispondrá para los usuarios. De este modo, a diferencia del modelo de patrocinio de servicios, este último modelo no implica un tratamiento discriminatorio respecto del contenido, las aplicaciones y los servicios, debido a que los usuarios son libres de utilizar los datos patrocinados con el propósito que deseen. Así, el patrocinio de datos independiente de las aplicaciones es totalmente compatible con la neutralidad de la red. Como ejemplos de dicho modelo se pueden mencionar el proyecto Equal Rating de Mozilla, la aplicación mCent o la oferta de Free Basic internet propuesta por el operador de la India Aircel. La iniciativa de Mozilla se ha experimentado en distintos países de África. En base a la asociación con el operador de telecomunicaciones Orange, el proyecto se propone ofrecer un *smartphone* de 40 dólares con el sistema operativo Firefox y texto ilimitado, conversaciones y 500 MB de datos por mes durante seis meses.[52] Por otro lado, la aplicación mCent se basa en un innovador modelo de negocios que premia, con una cantidad de datos determinada, la participación de los usuarios en una variedad de actividades tales como "descargar datos y utilizar aplicaciones, responder encuestas, mirar videos, suscribirse a un servicio y/o participar en concursos".[53] Por último, el operador Aircel ha decidido ofrecer un límite de datos de 500 MB a todas las nuevas activaciones prepagas durante un período

[51] Belli, *supra* nota 41.

[52] Dixon-Thayer, Denelle, "Mozilla View on Zero-Rating", The Mozilla Blog, 5 de mayo de 2015. Disponible en: https://mzl.la/1RbY81R.

[53] *Véase* mCent, http://bit.ly/2glOcZ1.

de 90 días, con vigencia desde la fecha de activación.[54] Aunque dichos planes se pueden categorizar como ofertas de *zero-rating*, pareciera evidente que su objetivo no es ni favorecer ni perjudicar contenido, aplicaciones o servicios específicos, por lo que los datos patrocinados independientes de las aplicaciones parecieran ser totalmente compatibles con la neutralidad de la red.

III. El Marco Civil de Internet: abordaje brasileño de la neutralidad de la red y el *zero-rating*

El Marco Civil (MCI) es el marco de derechos humanos encargado de definir la base jurídica de la regulación de internet en Brasil. A pesar de su categoría de ley ordinaria, el MCI ha sido considerado como la "Constitución de Internet" de Brasil, dado que define los elementos fundacionales de la disciplina de internet en Brasil como también su marcada intención de proteger los derechos y libertades fundamentales en la web. El MCI se considera el ícono internacional de la democracia participativa debido al proceso de consulta en línea que llevó a su creación. El proceso de apertura y colaboración que condujo a la creación del MCI se inició y orquestó conjuntamente con el Centro de Tecnología y Sociedad de la Fundação Getulio Vargas junto con el Ministerio de Justicia de Brasil[55]. El ex presidente Luiz Inácio Lula da Silva promovió el MCI con el compromiso de desarrollar un "marco de derechos civiles para internet"[56] y recibió un fuerte respaldo de la presidente Dilma Rousseff. En respuesta a las revelaciones de inteligencia por parte del ex contratista de la NSA e informante, Edward Snowden, Rousseff llamó a la implementación de fuertes garantías de los derechos humanos en la web tanto a nivel internacional como nacional. Por lo tanto, el MCI fue el resultado de la combinación de democracia participativa y la firme voluntad política de proteger la "libertad de expresión, la privacidad del individuo y el respeto por los derechos humanos" mientras se garantiza la "neutralidad de la red, guiada únicamente por criterios técnicos y éticos, considerándose inadmisible su restricción por razones políticas, comerciales, religiosas u otras"[57]. En este

[54] La propuesta denominada Free Basic Internet no debe confundirse con la iniciativa Free Basics de Facebook.

[55] *Véase*, Brazilian Internet Steering Committee (CGI.br), "Um pouco sobre o Marco Civil da internet", 20 de abril de 2014. Disponible en: http://bit.ly/2fQpL3E.

[56] Véase Mário Coelho, "Lula quer regular a internet", *Congresso em Foco*, 24 de noviembre de 2009. Disponible en: http://bit.ly/2eVJ2l3.

[57] *Véase*, la declaración de H.E. Dilma Rousseff, presidente de la República Federativa de Brasil, en la 68va Sesión de la Asamblea General de las Naciones Unidas, 24 de septiembre, 2013.

sentido, el relator del MCI en la Cámara de Diputados, Alessandro Molon, argumentó que la neutralidad de la red es un derecho fundamental y la piedra angular de la democracia, que le permite a los individuos tener acceso a una pluralidad de fuentes de información[58]. De ese modo, la consagración de la neutralidad de la red en la legislación brasileña señala el entendimiento del legislador de que el tratamiento no discriminatorio del tráfico de internet se ha vuelto un requisito previo fundamental para lograr democracias que funcionen correctamente, impulsadas por la pluralidad de la información, ideas, opiniones e innovación.

Es importante destacar que la NR se ha defendido en Brasil desde 2009, cuando el Comité Gestor de Internet de Brasil[59], más conocido por su sigla CGI.br, incorporó la neutralidad de la red en su decálogo de principios fundamentales de la gobernanza de internet. La definición de neutralidad de la red según el decálogo, que establece que "el filtrado y los privilegios de tráfico deben sujetarse únicamente a criterios técnicos y éticos, siendo inadmisibles motivos políticos, comerciales, religiosos, culturales o cualquier otra forma de discriminación o favoritismo"[60], se reformuló repetidas veces durante el proceso de elaboración del MCI[61], hasta que se aprobó su versión final en abril de 2014. Finalmente, la neutralidad de la red se consagró en el MCI e impuso "el deber del operador de procesar, de manera isonómica, todo paquete de datos, independientemente del contenido, el origen y el destino, el servicio, la terminal o la aplicación"[62]. De manera importante, el MCI incluyó explícitamente la neutralidad de la red entre los principios que definen "la disciplina del uso de internet en Brasil"[63], junto con derechos fundamentales tales como la privacidad y la libertad de expresión, destacando la función instrumental de dichos principios "a fin de promover (i) el derecho de todos de acceder a internet; (ii) el acceso a la

[58] *Véase*, "Molon defende neutralidade da rede e critica qualidade da internet brasileira em Conferência Internacional da FGV-Rio", 11 de junio de 2015, disponible en: http://bit.ly/2fQtApt.

[59] El Comité Gestor de Internet de Brasil es un organismo que cumple varias funciones destinadas a "coordinar e integrar todas las iniciativas de servicios de internet en Brasil y promover la calidad técnica, la innovación y la diseminación de los servicios disponibles". *Véase*, http://bit.ly/2fQzlhJ.

[60] Véase, "Los principios para la gobernanza y el uso de internet". Disponible en: http://bit.ly/2fL3jlO.

61 Ramos, Pedro Henrique Soares, "Arquitetura da rede e regulação: a neutralidade da rede no Brasil", Fundación *Fundação Getulio Vargas*, Escuela de Derecho, San Pablo, 2015. Disponible en: http://bit.ly/2fPlD1c.

[62] *Véase*, Marco Civil, art 9.

[63] *Véase*, Marco Civil, art 2.

información, al conocimiento y la participación en la vida cultural y en el manejo de los asuntos públicos; (iii) la innovación y el estímulo a la amplia difusión de las nuevas tecnologías y modelos de uso y acceso"[64]. Así, el MCI le asigna a la neutralidad de la red una posición primaria, colocándola entre los principios constitucionales tales como la protección de los derechos humanos y la promoción de la innovación, a fin de destacar el rol crucial de la neutralidad de la red para promover un entorno sostenible de internet.

El legislador brasileño ha considerado que la neutralidad de la red es necesaria para evitar el tipo de control que potencialmente pudiera limitar la capacidad de los usuarios de recibir e impartir información e ideas, incluida su capacidad de compartir innovación. En este sentido, el tratamiento no discriminatorio que contempla el principio de neutralidad de la red permite a los usuarios convertirse en desarrolladores activos de la innovación y productores de contenido además de ser meros consumidores, desatando así un círculo virtuoso de innovación[65], y creando un campo de juego equitativo para los emprendedores y las empresas a fin de que lancen productos y servicios innovadores. Por estos motivos, el MCI elige proteger firmemente la NR, permitiéndoles a los operadores administrar de forma discriminatoria el tráfico de internet siempre y cuando dicha administración sea "esencial para la adecuada provisión de los servicios y aplicaciones (o para la) priorización de los servicios de emergencia".[66] Más aún, mientras el MCI promueve "la libertad de los modelos de negocios"[67] en internet, especifica claramente que dicha libertad no podrá superar la neutralidad de la red, declarando que la oferta comercial no podrá "entrar en conflicto con los otros principios establecidos en esta ley". Como tal, en su artículo 9, el MCI sugiere que deben quedar prohibidas las prácticas fundadas en un tratamiento diferencial, tales como el *zero-rating*. Sin embargo, debido a que dicha disposición debía establecerse mediante decreto presidencial, los operadores comenzaron a ofrecer planes de *zero-rating* en el mercado brasileño, argumentando que el *zero-rating* no contradice la NR y aguardando las aclaraciones respectivas por parte de la normativa del MCI.

Entre fines de 2014 y comienzos de 2016, el ministro de justicia de Brasil organizó una consulta destinada a elaborar el decreto mediante un proceso

[64] *Ibíd*, art 4.

[65] Williamson, Brian, Black, David y Punton, Thomas, "The Open Internet. A Platform for Growth", un informe para la BBC, Blinkbox, Channel 4, Skype y Yahoo!, Plum Consulting, octubre de 2011. Disponible en: http://bit.ly/2fVt61F.

[66] *Ibíd*, art 9.

[67] *Ibíd* art. 3, VIII.

participativo. Al igual que en otros países, en Brasil, las partes interesadas han brindado respuestas bastante polarizadas respecto del *zero-rating*, mostrando una marcada división de puntos de vista. Por otro lado, los operadores y los fabricantes de equipos de redes respaldaron fuertemente la adopción de modelos de *zero-rating* al tiempo que todos los demás consultados argumentaron que el *zero-rating* debería considerarse incompatible con las disposiciones de la neutralidad de la red.[68] Es de destacar que quienes respaldan el *zero-rating* han declarado que dicha modalidad proporcionaría a los consumidores un acceso gratuito (es decir, subsidiado) a servicios, aplicaciones y contenido seleccionado, permitiéndoles a los consumidores que no poseen recursos poder acceder a ciertos servicios a los que de otro modo deberían renunciar. Por otro lado, los detractores del *zero-rating* han declarado que, en el largo plazo, los beneficios potenciales del *zero-rating* aparecerán a expensas del desarrollo del ecosistema digital brasileño y de la libertad de información y opinión de los ciudadanos de Brasil. A pesar de que el *zero-rating* puede considerarse un modelo de negocios legítimo, es importante recordar que el artículo 2 del MCI exige la firme protección de los derechos humanos, la pluralidad y la apertura, y el artículo 3 somete explícitamente "la libertad de los modelos de negocios" al respeto de "otros principios establecidos en esta ley", tales como la neutralidad de la red. Desde esta perspectiva, la consulta brasileña ha arrojado que el *zero-rating* se propone guiar a los usuarios hacia los servicios menos costosos en lugar de aquellos más innovadores o útiles, creando así muros que encierran a los usuarios de bajos recursos para que solo utilicen servicios y burbujas de información subsidiados y predefinidos por los operadores.

La consulta permitió la elaboración del decreto 8.771/2016[69] que proporciona una guía más amplia respecto de la ilegalidad del *zero-rating* dentro del sistema jurídico brasileño. Es de destacar que el artículo 9 del decreto del MCI prohíbe toda práctica que "comprometa el carácter público e irrestricto del acceso a internet y los elementos y principios fundacionales como así también los objetivos del uso de internet en el país" o "favorezca aplicaciones ofrecidas por aquellos responsables de la transmisión, conmutación o ruteo, o por empresas del mismo grupo económico". Sin embargo, es importante destacar que, hasta la fecha, los operadores brasileños han rechazado la incompatibilidad del *zero-rating* y de la neutralidad de la red,

[68] Brito Cruz, Francisco Carvalho et al., "What is at Stake in the Regulación of the Marco Civil?", informe final sobre el debate público, auspiciado por el Ministerio de Justicia en la regulación de la ley 12.965/2014, InternetLab, 2015. Disponible: http://bit.ly/1QZE8kP.

[69] *Véase* Decreto Nº 8.771, 11 de mayo de 2016. Disponible en: http://bit.ly/1TRNpKo.

incluyendo los servicios de *zero-rating* en una gran variedad de planes de datos. Más aun, es importante reiterar que, en Brasil, solo cuatro aplicaciones bien establecidas se ofrecen mediante *zero-rating*, a saber: Facebook, Twitter, WhatsApp y Deezer. De este modo, el panorama del *zero-rating* en Brasil ejemplifica de manera contundente las críticas según las cuales es probable que los planes de *zero-rating* consoliden a los actores bien establecidos en lugar de promover la competencia, el surgimiento de nuevos servicios y el pluralismo mediático. En rigor de verdad, como lo demuestra el ejemplo brasileño, solo los servicios populares resultan lo suficientemente atractivos y poseen el poder de negociación necesario para cerrar acuerdos de *zero-rating*. Más aun, dicho escenario confirma las críticas según las cuales el *zero-rating* tiene el potencial de transformar a los usuarios activos de internet en consumidores pasivos de aplicaciones, impulsando un cambio desde una internet de uso general y generadora de contenidos hacia una red estancada con un uso predefinido al estilo Minitel.[70]

Aunque el *zero-rating* puede considerarse como un método eficiente de brindar servicios patrocinados a los usuarios, pareciera incuestionable que se basa en la discriminación positiva de dichos servicios patrocinados con el objetivo de fomentar la creación de usuarios de servicios específicos en lugar de prosumidores de internet. Dicha evolución pareciera estar en franco conflicto con el artículo 3 del MCI, que establece "la preservación y garantía de la neutralidad de la red" como así también "la preservación de la naturaleza participativa de la red" como principios fundamentales de la disciplina de internet en Brasil. Más aún, al promover el uso de solo cuatro aplicaciones *zero-rating*, los planes no parecen ser compatibles con el respeto y la promoción de la "libre iniciativa, la libre competencia, (…) la pluralidad y diversidad" que están explícitamente definidos en el artículo 2 del MCI. Por lo tanto, la jurisprudencia bien podría aclarar la compatibilidad de la práctica de *zero-rating* existente con las disposiciones del MCI antes mencionadas y con el artículo 10, decreto 8.771/2016, según el cual:

> Las ofertas comerciales y los modelos de facturación del acceso a internet deben preservar una única internet que sea abierta, plural

[70] Belli, *supra* nota 41. La red Minitel era un sistema cerrado, especialmente popular en Francia durante la década de los noventa, en la que solo el operador podía decidir los servicios que estarían disponibles para los usuarios al tiempo que la agencia gubernamental francesa a cargo de las telecomunicaciones tenía el derecho de aprobar o desaprobar cualquier servicio de forma unilateral.

y diversa en su naturaleza y comprendida como medio para la promoción del desarrollo humano, económico, social y cultural, y que contribuya a construir una sociedad inclusiva y no discriminatoria.

Conclusión

El fundamento principal de la neutralidad de la red es mantener a la internet como un sistema abierto y descentralizado, cuya evolución la puedan modelar directamente los usuarios. Como he mencionado, varias ofertas de *zero-rating* pueden potencialmente infringir el fundamento básico de la neutralidad de la red y solo resultan útiles cuando se las combina con límites de datos suficientemente bajos para que un individuo pueda disfrutar del plan de datos gratuito de un servicio patrocinado. Esto significa que ante la ausencia de límites de datos o cuando los límites de datos son suficientemente abundantes, los consumidores no se inclinan a considerar las ofertas de *zero-rating*.[71] De este modo, las prácticas *zero-rating* pueden promover escasez artificial, alentando a los operadores a mantener un bajo límite de datos para atraer a los consumidores con servicios patrocinados. Tal como he señalado, a pesar de que algunos modelos de *zero-rating* pueden utilizarse como soluciones temporales para permitir que los individuos no conectados puedan comunicarse, es importante advertir que existen soluciones más sustentables. En especial, las políticas públicas deberían promover la conectividad plena, otorgándoles a los individuos el poder de crear y de compartir innovación, siendo prosumidores activos en lugar de consumidores pasivos. En este sentido, los formuladores de políticas deberían evaluar los costos y beneficios del *zero-rating* y también considerar soluciones alternativas tales como redes comunitarias.[72] Las redes comunitarias ya se encuentran presentes en varios países desarrollados y en vías de desarrollo y, a diferencia de los esquemas de *zero-rating*, se basan en el empoderamiento individual

[71] Arnold, R. y col., "The Value of Network Neutrality to European Consumers", estudio encargado por BEREC, abril de 2015. Disponible en: http://bit.ly/2f7apXc.

[72] Para consultar una reseña sobre redes comunitarias, *véase*, Belli (ed.), "Community Connectivity: Building the Internet from Scratch". Relatoría anual de la Coalición Dinámica sobre Conectividad Comunitaria del IGF, FGV Editor, 2016; Baig, R. y col., "Guifi.net, una infraestructura de red colaborativa", Competer Networks, 2015. Disponible en: http://bit.ly/1l5WVgr. Giovanella F. y Caso R. (eds.), "Reto di liberá. Wireless Comunista Networks: un'analisi interdisciplinare", Università Degli Studi di Trento, 2015; De Filippi, P. y Tréguer, F., "Wireless Community Networks: Towards a Public Policy for the Network Commons?", en Belli y De Filippi (eds.), *supra* nota 2.

mediante la creación de infraestructuras desde los extremos, a nivel del usuario. La característica más común de las redes comunitarias es el uso de las tecnologías de *networking* por y para la comunidad local: las implementa la comunidad local de individuos y organizaciones, y luego las administra dicha comunidad mediante recursos compartidos y esfuerzos coordinados.

Este abordaje no es meramente teórico, sino que ya ha demostrado la capacidad de producir beneficios concretos y distribuidos. Algunos ejemplos destacados incluyen la red Guifi.net[73] con sus más de 33.000 participantes diseminados en toda la región de Cataluña, España, y las redes comunitarias creadas por la asociación argentina AlterMundi,[74] y la Indian Digital Empowerment Foundation.[75] El objetivo principal de dicha red es empoderar a las comunidades a través de las tecnologías, permitiéndoles a los participantes desarrollar y administrar la infraestructura como un recurso común. Lo que es más importante, las redes comunitarias permiten ofrecer y recibir cualquier tipo de servicio de modo no discriminatorio y sin inspección o modificación de los flujos de datos dentro de la red más allá de lo estrictamente necesario para su operación.[76] Como tales, las redes comunitarias no solo son compatibles con los fundamentos de la neutralidad de la red, sino que además promueven el empoderamiento pleno del usuario, en especial porque están dirigidas a la población que no se encuentra conectada. En rigor de verdad, las redes comunitarias se basan en el uso de modelos de redes fáciles de implementar, que los individuos que carecen de conocimiento técnico pueden reproducir y explotar oportunamente. Dichos modelos de redes se basan en el uso de:

> Hardware de referencia basado en equipos hogareños inmediatamente disponibles; un diseño fácil de construir para antenas direccionales de banda dual; software (firmware) responsable de la configuración automática de nodos de redes y ruteo dinámico; una interfaz web para el manejo y la alineación de antenas; y una serie de herramientas para el monitoreo y el mapeo de redes.[77]

[73] *Véase*, http://bit.ly/2fpvl9r.

[74] *Véase*, http://bit.ly/2fPQlXk.

[75] *Véase*, http://bit.ly/2eVQpZZ.

[76] Echániz, Nicolás, "Comunista Networks: Internet from the First Mile", en *FRIDA: 10 Years Contributing to Development in Latin America and the Caribbean*, FRIDA Program, LACNIC, octubre de 2015. Disponible en: http://bit.ly/1Nt5aKr.

[77] *Ibíd.*

Como se observó en los apartados II y III, las prácticas de *zero-rating* pueden no ser compatibles con la neutralidad de la red y pueden limitar sustancialmente el modo en que los individuos utilizan y aprovechan la internet. Por su parte, las redes comunitarias parecen ofrecer una respuesta muy concreta a la búsqueda de la inclusión digital, dado que no solo cuentan con el potencial de crear infraestructura desde los extremos sino también de estimular la alfabetización digital, el empoderamiento comunitario y la creación de contenido y servicios locales. En una era en la que los gobiernos son frecuentemente criticados por carecer de visión política y priorizar los intereses de actores privados bien establecidos, la promoción de una conectividad sustentable mediante abordajes que empoderen a los usuarios, tales como redes comunitarias, sería la elección inteligente para restaurar la confianza tan necesaria en los formuladores de políticas, y proteger al mismo tiempo una internet no discriminatoria y centrada en el usuario.

Otras referencias

Comité de Derechos Humanos de Naciones Unidas, "La índole de la obligación jurídica general impuesta a los Estados Partes en el Pacto", Observación general No. 31, Reunión No. 2187, lunes 29 de marzo de 2004.

Federal Communications Commission (FCC), "Preserving the Open Internet", GN Docket No. 09-191, WC Docket No. 07-52, Report and Order, 25 FCC Rcd 17.905, 17.911, 2010.

Internet Society (ISOC), Lifting Barriers to Internet Development in Africa: suggestions for improving connectivity, 8 de mayo, 2013. Disponible en: http://bit.ly/1MRw17S.

Capítulo Cuatro

¿Se puede tener el oro y el moro? *Zero-rating*, neutralidad de la red y el derecho internacional

Arturo J. Carrillo[1]

Resumen ejecutivo

Este artículo analiza la respuesta que el derecho internacional le da al enigma del *zero-rating* (tasa cero). Los debates nacionales sobre la admisibilidad del *zero-rating*, que viola la neutralidad de la red, como medio para aumentar la conectividad se propagan en todo el mundo, particularmente en los países en vías de desarrollo. Por lo general, estas discusiones extremadamente polémicas carecen de rigor, objetividad e influencia. Se caracterizan por una colisión de dogmas: por un lado, la santidad de los principios de la neutralidad de la red, y por el otro, la obligación de cerrar la brecha digital o de respetar los mercados libres. Este artículo pretende salvar esa dicotomía al invocar el marco del derecho internacional aplicable para analizar el *zero-rating* como un límite sobre la neutralidad de la red entendida como norma de derechos humanos, algo que la neutralidad de la red demuestra ser. Según este punto de vista, el enigma del *zero-rating* se convierte en un conflicto de derechos más flexible –el derecho de brindar y recibir información de forma gratuita contra el derecho de acceder a internet– que puede analizarse

[1] Arturo Carrillo es profesor de Clínica Jurídica; Director de la Clínica Internacional de Derechos Humanos; Co-director del Global Internet Freedom y de Human Rights Project de la Escuela de Derecho de George Washington University. El autor agradece a Anupam Chander, Gene Kimmelman, Kevin Martin, Dawn Nunziato, Daniel O'Maley, Courtney Radsch y Carolina Rossini por sus comentarios. También agradece a los siguientes estudiantes de la Escuela de Derecho de George Washington University por su colaboración en la investigación: Ana González, Matthew Halldorson, Carrie James, Jannat Majeed, Nora Mbagathi, y Darke Zheng. "El presente artículo es una traducción del original en inglés. La versión en inglés ha sido publicada en Stanford Technology Law Review en octubre de 2016 (19 STAN.TECH. L.REV. 364 (2016)).

de manera constructiva mediante el régimen de excepciones que establece el derecho de los derechos humanos para resolver este tipo de conflictos. De conformidad con este marco, que vincula legalmente casi al 80% de los países del mundo, las excepciones propuestas para la neutralidad de la red, como el *zero-rating*, deberán examinarse según las condiciones específicas de cada país. Estas excepciones se evalúan mediante una prueba de equilibrio de factores, que incluye la necesidad y la proporcionalidad, para determinar si, en términos generales, la libertad de expresión se ve fomentada en ese contexto particular. Este enfoque tiene la ventaja adicional de poder aceptar aportes de otros campos, como la economía y las políticas de la tecnología. En resumen, se apunta a entender la forma en que se aplican las normas legales de derechos a la neutralidad de la red y al *zero-rating* debería, en la práctica, para así conducir a un discurso más fundamentado en ambas partes del debate y, por ende, a mejores resultados.

Introducción

Como consecuencia de los debates intensos sobre la neutralidad de la red en los Estados Unidos, que culminaron en la Norma sobre Internet Abierta 2015 emitida por la Comisión Federal de Comunicaciones (FCC, por su sigla en inglés),[2] la atención viró hacia debates sobre políticas similares en Europa y en el resto del mundo.[3] En India se está librando una batalla para proteger la neutralidad de la red, con consecuencias transcendentales. Allí, los entes reguladores del Gobierno debieron confrontar una reacción violenta de la sociedad en 2015 por los llamados planes de *zero-rating* (tasa cero) que ofrecían los operadores de redes móviles locales.[4] La unión de fuerzas entre una compañía de telecomunicaciones de India con Facebook, a principios de 2015, para implementar Internet.org –la plataforma en línea de Facebook (ahora denominada Free Basics)– con el objetivo de promover la conectividad en los países en vías de desarrollo fue el disparador de esa reacción. Entre otras cosas, Internet.org ofrecía acceso limitado a un con-

[2] Normas de protección y promoción de la internet abierta, 80 regulaciones federales, 19.738, 13 de abril de 2015 (a codificarse bajo el título 47 del Código de Regulaciones Federales, CFR pts. 1, 8, 20), disponible en http://bit.ly/2frYDqL (De aquí en adelante Norma sobre Internet Abierta 2015).

[3] *Véase*, por ejemplo, O'Reilly, Quinton, "The EU Has Plans for an Open Internet, but What Does it Mean?", *The Journal.ie*, 11 de julio de 2015, disponible en: http://bit.ly/2fKpYp0

[4] *Véase*, Arakali, Harichandan, "Facebook Square Off over Net Neutrality in India", *Int'l Business Times*, 17 de abril de 2015, disponible en: http://bit.ly/2eQejpl.

junto de contenidos y servicios selectos en línea en forma gratuita.[5] Otras empresas de internet, pequeñas y grandes, ofrecen acceso gratuito a internet móvil en muchos países en vías de desarrollo en todo el mundo.[6]

En los últimos años, varios gobiernos, incluso el de los Estados Unidos, han legislado protecciones sólidas sobre la neutralidad de la red para garantizar que la libertad de expresión y de pensamiento en línea no se vea distorsionada por las fuerzas del mercado o restringida de manera injusta por los proveedores de internet.[7] Una amenaza potencial a la neutralidad de la red es el *zero-rating*, que hace referencia a "la práctica realizada por los proveedores de servicios de internet donde ofrecen a sus clientes una gama específica de servicios o aplicaciones gratuitas sin sujeción a un plan de datos o a los límites existentes para datos".[8] Numerosos países están en proceso de implementar marcos regulatorios que determinarán en qué casos y en qué momento se permitirán restricciones sobre la neutralidad de la red, especialmente sobre *zero-rating*.[9] Sin embargo, ¿qué hay de malo en ofrecer un acceso a internet limitado pero gratuito para aquellos sectores de la población que probablemente de otro modo no podrían gozar de dicha conectividad o servicios?

Parece que resulta ser bastante malo. En primer lugar, el esquema *zero-rating* actúa como una restricción sobre la neutralidad de la red, el principio que establece que los proveedores de servicios de red –incluso los operadores de redes móviles– deben tratar todos los datos y contenidos en línea de forma

[5] Russell, Jon, "Facebook Takes Internet.org and its Free Mobil Data Services to India", *Tech Crunch*, 9 de febrero de 2015, disponible en: http://tcrn.ch/1z4fySt. *Véase además*, "'Free Basics by Facebook' Replaces Internet.org Website and App", Engadget, 24 de septiembre de 2015, disponible en: http://engt.co/2fPeHBX. Establece que Free Basics ofrece un menú de selección de servicios y aplicaciones a los usuarios en Asia, África y América Latina.

[6] Véase, *infra* Parte I.A.

[7] Véase, *infra* notas 228-244 y texto acompañante.

[8] *Véase*, por ejemplo, "Open Letter to Mark Zuckerberg Regarding Internet.org, Net Neutrality, Privacy, and Security", Facebook, 18 de mayo de 2015, disponible en: http://bit.ly/1L23He3 (De aquí en adelante, Carta abierta]. *Véase además*, Baker, Mitchell, *Zero Rating and the Open Internet*, Lizard Wrangling Blog, 6 de mayo de 2015, disponible en: http://bit.ly/1lLOGyz.

[9] *Véase*, por ejemplo, "Net Neutrality: DoT Panel Against Facebook's Internet.org, Favours Airtel Zero", *India Today*, 6 de julio de 2015, 10:13 horas, disponible en: http://bit.ly/2fVvc2C. *Véase además*, Marini-Balestra, Frederico, y Termolada, Ricardo, "The EU Debate on Net Neutrality: What about Zero Rating?", Academia, 2015, disponible en: http://bit.ly/2gK5U8Q; Rey, Patricia, "Net Neutrality in Mexico: Still a Long Way to Go", *BNamericas*, 27 de febrero de 2015, disponible en: http://bit.ly/2fl8XLG.

equitativa[10] para garantizar así el libre flujo de información y el acceso no restringido a dicha información.[11] Desde esta perspectiva:

> *Zero-rating* es (una) técnica discriminatoria a través de la cual las compañías de telecomunicaciones permiten que sus clientes accedan a una selección de contenido y servicio sin costo adicional alguno, mediante un acuerdo previo con los proveedores de contenido. Los clientes acceden a los sitios seleccionados de manera gratuita, y de esta manera violan la esencia de la neutralidad de la red que exige no discriminar entre contenidos y aplicaciones diferentes.[12]

En pocas palabras, como el *zero-rating* viola la neutralidad de la red por definición, la controversia gira en torno al hecho de si se debería permitir el *zero-rating*, y de ser así, en qué situaciones.[13] Esto es lo que denominamos el enigma del *zero-rating*. Hasta el momento, el enfrentamiento más intenso que involucra este enigma transcurre en India, donde los debates públicos han captado la atención a nivel internacional desde 2015.[14] El lanzamiento

[10] Relator especial de la ONU sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión; representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa; relator especial sobre la Libertad de Expresión de la OEA; y relator especial sobre la Libertad de Expresión y Acceso a la Información de la Comisión Africana de los Derechos Humanos y de los Pueblos (ACHPR, por su sigla en inglés). Declaración Conjunta sobre Libertad de Expresión en Internet de OSCE, 1 de junio de 2011, disponible en: http://bit.ly/1CUwVap (de aquí en adelante Declaración conjunta) *Véase*, Norma de Internet Abierta 2015, *supra* nota 2, en 1.

[11] Carta abierta, *supra* nota 8: "La neutralidad de la red respalda la libertad de expresión y la igualdad de oportunidades al permitir que las personas busquen, reciban y brinden información, y que interactúen como pares. Requiere que internet se mantenga como una plataforma abierta sobre la cual los proveedores de servicios de internet traten todos los contenidos, las aplicaciones y los servicios de manera equitativa, sin discriminación. Un aspecto importante de la neutralidad de la red establece que todos deberían poder innovar sin permiso de ninguna persona o entidad".

[12] Kiran Singh, Vipal, "Permit *Zero-Rating* Schemes for a Limited Period", *The Financial Express*, 9 de julio de 2015, disponible en: http://bit.ly/2eOOpz2.

[13] El debate sobre la política que circunda la neutralidad de la red en un país determinado irá mucho más allá que el mero hecho del *zero-rating*. Para un debate detallado de la mayoría (o de todas) de las consideraciones relevantes en ese análisis. *Véase*, Van Schewick, Barbara, "Network Neutrality and Quality of Service: What a Nondiscrimination Rule Should Look Like", 67 *Standford Law Review*, No. 1, 2015. Sin embargo, me enfocaré principalmente en el tema clave de *zero-rating* por los motivos mencionados en la presente Introducción.

[14] Véase, por ejemplo, Morozov, Evgeny, "Facebook Isn't a Charity. The Poor Will Pay by Surrendering Their Data", *The Guardian*, 25 de abril de 2015, disponible en: http://bit.ly/1DDtjtx.

de Internet.org en el mes de febrero de ese año desató olas de protestas en la sociedad civil de India y entre los activistas de derechos digitales en todo el mundo.[15] Les preocupaba que Facebook, una compañía multinacional con fines de lucro, llegara a ser –a través de su plataforma Internet.org– un "guardia" de internet para millones de usuarios de teléfonos móviles en los países en vías de desarrollo, con consecuencias nefastas para la innovación y la competencia local, así como para el desarrollo social.[16]

A medida que se desataba una reacción adversa hacia Internet.org en India, el CEO de Facebook, Mark Zuckerberg, respondía públicamente a las críticas en una columna de opinión publicada en un diario sobre finanzas en línea de India y en un mensaje publicado en su página de Facebook. Expresó que:

> Algunos han criticado el concepto de *zero-rating* que permite a Internet.org brindar servicios básicos de internet en forma gratuita, porque creen que juega en contra del espíritu de la neutralidad de la red. Discrepo rotundamente. Respaldamos absolutamente la neutralidad de la red con vehemencia. Queremos mantener internet abierta. La neutralidad de la red garantiza que los operadores de red no discrimen al limitar el acceso a los servicios que uno desea usar. Es una parte clave de la internet abierta, y estamos totalmente comprometidos con ello. Sin embargo, la neutralidad de la red no tiene conflictos con el hecho de buscar que más personas se conecten. Estos dos principios *–la conectividad universal y la neutralidad de la red– pueden y deben coexistir*.[17]

Los comentadores fueron rápidos al responder que Zuckerberg "no puede tener ambas cosas en términos de la neutralidad en la red".[18] Un periodista de Wired afirmó rotundamente que si la cuestión es "saber si el modelo de Internet.org se opone a los principios centrales de la neutralidad de la red, [la] respuesta [es] clara". Ambos son irreconciliables. Según esta postura, la pregunta que Zuckerberg y los defensores de *zero-rating* deberían responder es "si se deben aplicar las mismas reglas en aquellos lugares en donde las personas carecen de acceso a internet, sin mencionar

[15] *Ibíd*.

[16] Véase, *infra* notas 85-87 y texto acompañante.

[17] Zuckerberg, Mark, "Internet.org Does Not Violate Net Neutrality", *LiveMint*, 16 de abril de 2015, disponible en: http://bit.ly/1EQmXeK Facebook, 16 de abril de 2015, http://bit.ly/1znPO3S (con énfasis añadido).

[18] Lapowsky, Issie, "Mark Zuckerberg Can't Have it Both Ways on Net Neutrality", *Wired*, 17 de abril de 2015, disponible en: http://bit.ly/2fJc9tL.

un acceso equitativo".[19] La verdadera cuestión es si es aceptable "suspender algo del absolutismo de la neutralidad de la red que la comunidad tecnológica ha respaldado en los Estados Unidos en aras de un bien mayor para los países más pobres del mundo".[20] Asimismo, esto es una dimensión esencial del enigma de *zero-rating*.

Al insistir en que la "conectividad universal" y la neutralidad de la red "pueden y deben coexistir", Zuckerberg y Facebook están acusados de querer "tener el oro y el moro". Este proverbio intenta explicar que el objetivo ostensible –respeto total por la neutralidad de la red– y el resultado deseado –una plataforma de conectividad global basada en *zero-rating*– son incompatibles por naturaleza. Si uno se suscribe al "absolutismo de la neutralidad de la red" que caracteriza a ciertos sectores de los debates sobre neutralidad de la red en los Estados Unidos, entonces esa conclusión es inevitable. Pero ¿la neutralidad de la red como principio es absoluto realmente? Las cuestiones reflejadas en el debate precedente muestran consecuencias que traspasan las fronteras de cualquier país.

Otros proveedores de servicios de internet, compañías de telecomunicaciones y gobiernos en todo el mundo han seguido de cerca el desarrollo de las contiendas regulatorias sobre la neutralidad de la red en India, Europa y en otros lugares.[21] Finalmente, el ente regulador de India decidió prohibir la fijación de precios diferenciales, incluso el *zero-rating*, por parte de las compañías de telecomunicaciones en febrero de 2016.[22] En los Estados Unidos, la Comisión Federal de Comunicaciones adoptó una serie de medidas de protección contundentes respecto de la neutralidad de la red que, sin

[19] *Ibíd*.

[20] *Ibíd*.

[21] *Véase*, por ejemplo, Autoridad Regulatoria de Telecomunicaciones de India (TRAI), "Consultation Paper on Differential Pricing for Data Services", en 9, 9 de diciembre de 2015, disponible en: http://bit.ly/1JrDlkw (de aquí en adelante TRAI Consultation Paper; McCarthy, Kieren, "Council of Europe Gets Tough on Net Neutrality: No Blocking, Slowing Down, Degrading or Discriminating of internet Traffic", *The Register*, 13 de enero de 2016, disponible en: http://bit.ly/2gPqDEA (de aquí en adelante el "Consejo de Europa se posiciona duramente respecto de la neutralidad de la red"). Brasil es un ejemplo de otra línea de fuego en esta contienda. *Véase*, Brito Cruz, Francsico, y Coelho Marchesan, Jonas, "Net Neutrality in Brazil: The Debate Continues", *InternetLab*, 4 de febrero de 2016, disponible en: http://bit.ly/2gYJTUj.

[22] *Véase*, Gowen, Annie, "India Bans Facebook's 'Free' internet for the Poor", The Washington Post, 8 de febrero de 2016, disponible en: http://wapo.st/1W6GX28; Hempl, Jesse, "India Bans Facebook's Basics App to Support Net Neutrality", *Wired*, 8 de febrero de 2016, disponible en: http://bit.ly/2fVzdnM. *Véase*, *además*, Parte III.B. (debate sobre acontecimientos recientes en India).

embargo, han dejado abierta la puerta a planes "con datos patrocinados" por *zero-rating*, siempre y cuando no presenten una desventaja injusta o irrazonable en lo que respecta a la selección y expresión de los consumidores.[23] Lo que esto significa son meras suposiciones.

Sin importar desde dónde se lo mire, hay mucho en juego en el debate sobre *zero-rating*. Pero cómo uno lo mire es fundamental para abordar la tensión inherente entre la neutralidad de la red y el *zero-rating* de manera coherente. Este artículo aborda la cuestión mediante una "nueva" perspectiva sobre el debate: el derecho internacional de los derechos humanos. Por supuesto que este conjunto de normas no es nuevo. No obstante, en la mayoría de los países, la polémica que gira alrededor de la regulación sobre *zero-rating* y la neutralidad de la red, en gran medida, carece de referencias a las normas sobre derechos humanos. Los debates sobre políticas se han concentrado en las dimensiones sociales, económicas y técnicas del *zero-rating*, como lo demuestra el cuerpo de investigación, modesto, pero en constante desarrollo, así como los comentarios sobre este tema.[24] Pero, aunque los defensores posicionados en ambos bandos del debate intensifican la búsqueda de mejores datos empíricos, su consideración sobre el marco "regulatorio" del derecho de los derechos humanos sigue siendo transitoria en el mejor de los casos. Este artículo pretende darle un nuevo marco a esa perspectiva y, de ser posible, expandirla.

---

[23] Véase *infra* notas 228-245 y texto acompañante.

[24] *Véase*, por ejemplo, "Session Report: WS 208: Net Neutrality, Zero-Rating, and Development", 9º Foro para la gobernanza de internet, Estambul, 3 de septiembre de 2014, disponible en: http://bit.ly/2eWzltV. Estudios recientes han comenzado a llenar los vacíos en la falta de datos empíricos. *Véase*, por ejemplo, "Center for Deliberative Democracy. Increasing Internet Access to the Next Billion", 2015 (de aquí en adelante "Estudio de Stanford"). *Véase además*, Smith, Alex, y Moskowitz, Ben, "Mobile for Development Impact: Approaches to Local Content Creation. Realizing the Smartphone Opportunity", 2015, disponible en: https://mzl.la/29P9WZZ (de aquí en adelante "Estudio sobre Mozilla"); Thakur, Dhanaraj, "The Impacts of Emerging Mobile Data Services In Developing Countries", Alliance For Affordable Internet, noviembre de 2015, disponible en: http://bit.ly/2fVqZvZ. Chair, Chenai, "Africa Supply Side Assessment of Zero Rating", Research ICT Africa, 10 de noviembre de 2015, disponible en: http://bit.ly/2fUkcmN. Soares Ramos, Pedro Henrique, "Towards a Developmental Framework for Net Neutrality: The Rise of Sponsored Data Plans in Developing Countries", TPRC Conference, 31 de marzo de 2014, disponible en: http://bit.ly/1gXJYmV. Layton, Roslyn, y Elaluf Calderwood, Silvia, "Zero Rating: Do Hard Rules Protect or Harm Consumers and Competition? Evidence from Chile, Netherlands and Slovenia", 15 de agosto de 2015, disponible en: http://bit.ly/2cevayH (de aquí en adelante Layton y Elaluf-Calderwood); Rossini, Carolina, y Moore, Taylor, "Exploring Zero-Rating Challenges: Views from Five Countries", Public Knowledge, documento de trabajo, julio de 2015, disponible en: http://bit.ly/2fRjbtB (de aquí en adelante, el Informe Public Knowledge de Rossini y Moore).

Cuando se analiza la neutralidad de la red como norma de los derechos humanos, algo que puede probarse. La cuestión del *zero-rating* adopta una nueva dimensión, que resulta fundamental para comprender la función propia de la neutralidad de la red en el mundo real. El enigma del *zero-rating* deja de ser catalogado como una dicotomía divisiva de dogmas y se transforma en algo más dócil: un conflicto de derechos, del tipo que se confronta y resuelve de manera regular dentro del marco del derecho internacional de los derechos humanos.[25] Cuando se lo analiza desde la mirada de los derechos humanos, "preservar la neutralidad [de la red] significa preservar la facultad de las *personas* para tomar decisiones sobre cómo usar internet –qué información buscar, recibir o brindar, desde qué fuentes y a través de qué servicios–".[26] Por consiguiente, la cuestión desde el punto de vista de los derechos humanos es la siguiente: ¿puede el *zero-rating* ser consistente con los principios de la neutralidad de la red, entendida como la libertad que tienen las personas de buscar, recibir y brindar información de manera no discriminatoria? Porque incluso los derechos fundamentales no son absolutos, la respuesta a esa pregunta es *sí, algunas veces, bajo ciertas circunstancias*.

El resto de este artículo está dedicado a examinar la neutralidad de la red como norma de derechos humanos y las condiciones bajo las cuales este principio puede ser calificado en forma legítima por las restricciones propuestas, como el *zero-rating*.

Se divide en tres partes. La Parte I evalúa el escenario de *zero-rating* a nivel internacional para establecer un cimiento para los análisis de carácter legal y político que continúa en las Partes II y III, respectivamente. En primer lugar, revisa las formas principales adoptadas por el *zero-rating* y ofrece una tipología de trabajo para facilitar el debate de las cuestiones pertinentes. Posteriormente, la Parte I analiza la neutralidad de la red y el *zero-rating* a lo largo de un rango de países representativos por región a través de métodos tanto cuantitativos (análisis estadísticos) como cualitativos (estudio de casos). La Parte II describe y analiza el marco normativo conforme al derecho internacional de los derechos humanos, poniendo especial énfasis en la libertad de expresión y en los principios de la no discriminación. Explora los orígenes del principio de la neutralidad de la red para entender su evolución, así como su relevancia como

[25] Véase, *infra* notas 246-331 y texto acompañante.

[26] "The Importance of internet Neutrality to Protecting Human Rights Online", Center for Democracy & Technology, No. 5, 2013, disponible en: http://bit.ly/2gcxAEb (de aquí en adelante Informe del CDT de 2013) (con énfasis añadido). La neutralidad de la red es algo fundamental para preservar la diversidad de los medios y el pluralismo en internet. Esto se debate en *infra* Parte II.B.I.

norma contemporánea de derechos humanos. Para finalizar, la Parte III aplica el marco legal de los derechos humanos al *zero-rating* en vistas de los datos precedentes con el propósito de demostrar cómo los formuladores de políticas, defensores, académicos y otros pueden utilizar esta "nueva perspectiva" para evaluar aún mejor la función y el impacto del *zero-rating* en contexto.

I. El escenario: *zero-rating* en el mundo

Esta segunda parte se divide en dos secciones. La sección A, que examina el escenario global del *zero-rating*. Comienza con un panorama general sobre las diversas formas que adopta el *zero-rating* y, en aquellos casos que resultan pertinentes, sobre los patrocinadores principales de esas iniciativas. Esto permite una diferenciación útil entre las diversas formas de las actividades pretendidas por el *zero-rating* vigentes o bajo estudio. Esta primera sección actúa como fondo de la segunda sección, que adopta una mirada cuantitativa y cualitativa de las condiciones bajo las cuales se implementan las políticas de la neutralidad de la red en diferentes países y regiones. La sección B compila los indicadores estadísticos clave para una muestra de los países seleccionados por región. Estos indicadores dan un panorama del desarrollo económico, social y político de cada país, especialmente en función del acceso fijo y móvil a internet. Por último, la sección B analiza las barreras a la conectividad que existen en estos y en otros países antes de describir los tres casos de estudio que ejemplifican los abordajes predominantes del *zero-rating*.

I.A. El escenario global: tipos de *zero-rating* y sus patrocinadores

Esta sección examina las configuraciones principales del *zero-rating* tal como se presenta en la actualidad. A modo de recordatorio, hemos definido *zero-rating* como la práctica que ofrece libre acceso a determinados servicios y datos en línea a clientes de redes móviles específicas.[27] Generalmente, esto

[27] Shears, Matthew, "No. 208 Net Neutrality, Zero-Rating & Development: What's the Data?", Internet Governance Forum, disponible en: http://bit.ly/2fcXYch. Cabe destacar que esta tipología no incluye el *zero-rating* de servicio público, como los utilizados por algunos gobiernos a los fines de emergencias u otros servicios públicos. A modo de ejemplo tenemos el gobierno regional del estado de San Pablo, en Brasil, que subsidia los servicios de gobierno electrónico a través de una plataforma *zero-rating* patrocinada de forma pública. *Véase*, Medeiros, Henrique, "Poupatempo no celular: acesso patrocinado custará r$20 milhões ao ano para o estado de SP", *TeleTime*, 28 de septiembre de 2015, disponible en: http://bit.ly/2gdxKKM *Véase además*, PoupaTempo, http://bit.ly/2fVzFBc (sitio web de servicios electrónicos del gobierno regional de San Pablo).

se implementa liberando el tráfico a ciertos sitios o a través de aplicaciones selectas a partir de límites a los datos del abonado al servicio.[28]

Asimismo, en algunos acuerdos relativos al *zero-rating*, los usuarios pueden tener acceso al servicio incluso aunque no cuenten con un plan de datos.[29] Estos tipos de programas son populares en el mercado de las redes móviles debido al costo elevado del ancho de banda si se lo compara con la internet alámbrica, sumado a la disponibilidad baja o inexistente de las conexiones con cables en muchos países.[30] El objetivo de esta sección es presentar una tipología funcional de las prácticas del sector privado respecto del *zero-rating* que pueden facilitar los siguientes análisis.

En este sentido, existen al menos cuatro modelos de prácticas de *zero-rating*: *zero-rating* de sitio o servicio único, datos patrocinados, *zero-rating* compuesto, y *zero-rating* falso (o no selectivo). Estas categorías no son mutuamente exclusivas: un determinado plan o una plataforma pueden incluirse en más de una categoría según sus características. A continuación, se examinará cada una de las categorías.

I.A.I. *Zero-rating* de sitio o servicio único

En un *zero-rating* de sitio o servicio único, una de las primeras formas adoptadas, un proveedor de contenido contrata a una o más compañías de telecomunicaciones para que brinde a los usuarios acceso libre a una versión de su sitio o servicio particular sin costo alguno. En general, el contenido basado en *zero-rating* puede ser exento de los "límites" del plan de datos del cliente o se puede acceder de forma totalmente separada de un plan de datos. A diferencia de los planes de datos patrocinados (que se debaten más adelante), los planes de sitios o servicios únicos quizás no necesiten que los proveedores de contenido paguen a la compañía de telecomunicaciones por el uso de datos basados en *zero-rating* por parte del cliente, si bien pueden hacerlo. Esos sitios pueden ofrecerse como un servicio de interés público sin fines de lucro, por ejemplo, Wikipedia Zero, o como un portal a internet mayor

[28] *Ibíd*.

[29] *Ibíd*. Los usuarios generalmente deben brindar algunos datos personales para suscribirse a los servicios o al sitio web de *zero-rating*, por lo que, en ese sentido, no son del todo "gratuitos".

[30] Drossos, Antonios, Rewheel, "Forget Fast Lanes. The Real Threat for Net-Neutrality Is Zero-Rated Content", Gigaom, 26 de abril de 2014, disponible en: http://bit.ly/2fRpJIA. *Véase*, Talbot David, "Around the World, Net Neutrality Is Not a Reality", MIT Technology Review, 20 de enero de 2014, disponible en: http://bit.ly/1yS5T1o (los usuarios no tienen acceso fácil a wifi y a conexiones no tradicionales en el hogar).

donde se puede acceder a sitios adicionales mediante el pago de una tarifa, por ejemplo, Google Free Zone. Otro ejemplo de una aplicación de servicio único que las compañías de telecomunicaciones ofrecen con *zero-rating* en varios países como una estrategia de mercado es WhatsApp, la aplicación para envío de mensajes más popular en todo el mundo.[31] Los proveedores de servicio de telecomunicaciones se benefician de estos acuerdos atendiendo a los usuarios que desean utilizar sitios o servicios gratuitos (y a través de pagos realizados por proveedores de contenido donde los hubiera) e incentivándolos a pagar por paquetes de datos o el uso de datos complementarios.

Los mejores ejemplos de *zero-rating* de sitio único son Wikipedia Zero, Google Free Zone y Facebook Zero, a pesar de haber diferencias importantes entre ellos. Wikipedia Zero es una iniciativa benéfica por parte de Wikimedia Foundation que, junto con los operadores de redes móviles, brindan acceso gratuito a Wikipedia para todos.[32] Su objetivo es "empoderar a las personas en todo el mundo para que desarrollen y compartan contenido educativo distribuido en forma gratuita".[33] Actualmente, está disponible en 57 países donde brinda acceso a tasa cero a sitios web accesibles a tales efectos a través de 75 operadores diferentes, y llega a 600 millones de personas aproximadamente.[34] Único entre los programas de zero-rating, Wikipedia Zero se compromete públicamente a brindar transparencia y responsabilidad a través de diez principios operativos.[35] Entre esos principios se incluyen: (1) los operadores deben proporcionar acceso basado en zero-rating a todas las partes de Wikipedia y no solamente a una parte del sitio; (2) los operadores deben garantizar que los usuarios no incurran de manera equivocada en gastos por datos y que sean notificados cuando estén por salir de un sitio con *zero-rating*; (3) no habrá intercambio de pago entre Wikipedia Zero y el operador del servicio móvil por el suministro de servicios de zero-rating; y (4) no existen los contratos

[31] WhatsApp 4, disponible en: http://bit.ly/2fcSwGr, Varias compañías de telecomunicaciones ofrecen WhatsApp a tasa cero como estrategia de mercado en Colombia, Ecuador, México y Brasil. Véase, Karisma Foundation, "¿Cómo se contrata en Latinoamérica el acceso a internet? ¿Qué tiene que ver esto con la neutralidad de la red?", No. 29, Año 34, 2016, disponible en: http://bit.ly/1slr7Ci. Informe de Public Knowledge de Rossini y Moore, *supra* nota 24, en 39-40.

[32] The Wikimedia Foundation, "Wikipedia Zero", disponible en: http://bit.ly/19HwmHD, último acceso: 3 de abril de 2015; "Mobile Partnerships", disponible en: http://bit.ly/2gpOy0H, último acceso: 30 de marzo de 2016.

[33] The Wikimedia Foundation, "Wikipedia Zero Operating Principles", disponible en: http://bit.ly/2gMk3jC, último acceso: 3 de abril de 2015.

[34] "Wikipedia Zero", *supra* nota32. *Véase*, *además*, "Mobile Partnerships", *supra* nota 32 (enumera los países anfitriones y las compañías de operadores móviles).

[35] *Véase*, "Wikipedia Zero Operating Principles", *supra* nota33.

exclusivos, el hecho de que un operador firme contrato con Wikipedia Zero no impide que otros operadores hagan lo mismo.[36]

Google ofrece otro plan con zero-rating de sitio único. Google Free Zone es una iniciativa que brinda a sus clientes acceso libre a Gmail, Google Search y Google Plus, el servicio de redes sociales para empresas.[37] Los clientes pueden acceder en forma gratuita a Gmail y a Google Plus desde sus teléfonos móviles, pero las funciones más avanzadas como la descarga de los adjuntos en correos electrónicos requieren de un plan de datos.[38] Asimismo, los clientes pueden buscar en Google a través de sus teléfonos sin incurrir en gasto alguno por datos.[39] La función Google Search les permite a los usuarios acceder a cualquier sitio web que aparece en la primera página de los resultados de la búsqueda realizada en Google Search, sin costo alguno.[40] Si los usuarios quieren acceder a sitios web no incluidos en los resultados de Google, deberán adquirir un plan de datos.[41] Debido a que Google Free Zone brinda, efectivamente, acceso basado *zero-rating* a contenido externo al cual se accede a través de los resultados del buscador, se puede considerar que goza de ciertas características de los planes de *zero-rating* compuesto, que se analizan más adelante.[42]

Facebook Zero –que no debe confundirse con Internet.org, la iniciativa de Facebook–[43] es un plan diseñado para permitir que los usuarios accedan a una versión limitada de Facebook en internet a través de su teléfono móvil en cualquier momento, sin cargo.[44] Los teléfonos inteligentes y los teléfonos básicos pueden acceder a Facebook Zero a través de la web o de una aplicación popular. En teléfonos no inteligentes, donde se lo optimiza, se le presenta al

[36] *Ibíd*.

[37] Press Trust of India, "Airtel Ties up with Google to Offer Free Search, Google+ and Gmail Services", Gadgents360, 26 de junio de 2013, disponible en: http://bit.ly/2gdvt2b. Google Free Zone se ofrece en las Filipinas, Sri Lanka, India, Tailandia, Nigeria y Kenia. *Véase*, "Reduce Data Usage on Android, iOS and Desktop", *So into Tech*, 16 de noviembre de 2014, disponible en: http://bit.ly/2gpMUMx.

[38] *Ibíd*.

[39] *Ibíd*.

[40] *Ibíd*.

[41] *Ibíd*.

[42] Mott, Nathaniel, "Google Debuts Free Zone to Challenge Facebook for Dominance in Developing Countries", *Pando*, 8 de noviembre de 2012, disponible en: http://bit.ly/2fCsvRo.

[43] Véase, infra notas 83-90 y texto acompañante.

[44] Wauters Robin, "Facebook Launches Zero, a Text only Mobile Site for Carriers", *TechCrunch*, 16 de febrero de 2010, disponible en: http://tcrn.ch/2fUAjkA.

usuario una versión reducida del sitio de redes sociales, con texto solamente.[45] Lanzado en mayo de 2010, Facebook se asoció con más de 50 operadores de telecomunicaciones para brindar acceso gratuito a Facebook Zero en 45 países.[46] Facebook no paga a sus socios de telecomunicaciones por proveer el servicio ni tampoco utiliza publicidad.[47] Facebook Zero está disponible para aquellos usuarios que tengan un plan de datos con uno de los proveedores asociados de servicios de telecomunicaciones.[48] Si un usuario desea acceder a fotografías o seguir vínculos externos, recibe una notificación que explica que incurrirán en cambios de datos si lo hacen.[49] Existe evidencia de que ocurre en muchos casos.[50] Asimismo, las personas que acceden a Facebook Zero pueden invitar a sus amigos para que lo hagan también, de esta manera llevan nuevos clientes al proveedor de telecomunicaciones.[51]

Al compararlo con otras formas de *zero-rating*, especialmente con los datos patrocinados y el *zero-rating* puro, estos planes de sitios o servicios únicos no han generado casi controversia. Aun así, tanto Google como Facebook han sido criticados por actuar como los "guardias" de internet para los millones de usuarios que acceden exclusivamente a través de sus sitios a tasa cero.[52] Tampoco ayuda el hecho de que en muchos lugares del mundo en vías de desarrollo, los planes de sitio único como Facebook Zero han llevado a ideas equivocadas y alarmantes en las mentes de millones de usuarios sobre qué es y qué no es internet.[53] Como respuesta directa a los planes de servicio único que ofrecen Facebook y Wikipedia, Chile se convirtió en el primer país en adoptar las normas de neutralidad de la red que prohíben esos

[45] Mims, Christopher, "Facebook's Plan to Find its next Billion Users: Convince Them the Internet and Facebook Are the Same", *Quartz*, 24 de septiembre de 2012, disponible en: http://bit.ly/2gPp35w.

[46] *Ibíd*.

[47] Véase, Mims, *supra* nota45.

[48] Véase, Wauters, *supra* nota44.

[49] *Ibíd*.

[50] "One Year in: Internet.org Free Basic Services", Internet.org, 27 de julio de 2015; Mozilla Study, *supra* nota24, en 12; Stanford Study, *supra* nota24, en 5; West, Darrell M., "Digital Divide: Improving Internet Access in the Developing World through Affordable Services and Diverse Content, 2 febrero de 2015, disponible en: http://brook.gs/2f1egHp.

[51] *Véase*, Wauters, *supra* nota44.

[52] Mott, *supra* nota 42.

[53] Mirani, Leo, "Millions of Facebook Users Have No Idea They're Using the Internet", *Quartz*, 9 de febrero de 2015, disponible en: http://bit.ly/2fJmna6. De 699 encuestados en Nigeria e Indonesia que utilizan Facebook Zero, casi el 10% (68) dijo que utilizan internet.

planes de manera rotunda,[54] si bien luego se retractó sobre Wikipedia Zero.[55] Además de violar los principios de la neutralidad de la red, estos planes de sitio único fueron criticados en Chile por representar "burbujas creadas por compañías como Google y Facebook para garantizar que sus productos sean sinónimo de 'la internet' en la mente de los usuarios".[56]

I.A.II. Datos patrocinados

En este modelo, los proveedores de contenido firman contratos y pagan a los proveedores de telecomunicaciones para ofrecer a los usuarios un abanico de información o servicios sin costo alguno. El ejemplo más conocido podría ser el servicio de datos patrocinados que ofrece AT&T. El programa de AT&T, lanzado en enero de 2014, permite que los anunciantes patrocinen datos móviles para sus suscriptores.[57] Ese patrocinio además permite que las compañías patrocinen "el uso de datos relacionados con las actividades comerciales de una empresa por parte de [sus] empleados o datos patrocinados como parte de un programa de fidelidad al cliente".[58] Las compañías de telecomunicaciones están patrocinando planes de datos patrocinados similares en otros países también. En 2015, una compañía de telecomunicaciones de India, Bharti Airtel, lanzó una plataforma de servicios con zero-rating, Airtel Zero, algo que generó polémica.[59] Esta plataforma ofrecía a los suscriptores acceso a un abanico de sitios y servicios locales cuyos proveedores pagaban a Airtel para estar incluidos.[60] De manera alternativa, la compañía de telecomunicaciones podría ofrecer el patrocinio

[54] Walker, Lauren, "How Is Net Neutrality Working for the Countries That Have It?", *Newsweek* (10 de septiembre de 2014), disponible en: http://bit.ly/1lWlkov. Véase además, *infra* notas 202-222 y texto acompañante.

[55] Informe Public Knowledge de Rossini y Moore, *supra* nota24, en 19.

[56] Mott, Nathaniel, "Chile Should Be Commended for Taking away Facebook and Wikipedia", *Pando*, 30 de mayo de 2014), disponible en: http://bit.ly/2fVzzdT.

[57] Bergen, Mark, "Net Neutrality Likely to Permit Sponsored Data Plans", Advertising Age, 12 de febrero de 2015, disponible en: http://bit.ly/2fPrnsr. Los datos patrocinados pueden adoptar diversas formas, incluso anuncios, juegos, aplicaciones comerciales o contenido. *Véase*, Strategy Analytics, "Sponsored Data not Hurt by Net Neutrality", "Benefits Consumers Says Strategy Analytics", *PR Newswire*, 11 de marzo de 2015, disponible en: http://prn.to/2eWX56A.

[58] Brandom, Russell, "Sponsored Data: AT&T Will Now Let Companies Buy out your Data Charges for Specific Videos and Apps", *The Verge*, 6 de enero de 2014, disponible en: http://bit.ly/1bLhMJO.

[59] "CEO Defends Airtel Zero Despite Backlash", *Times of India*, 18 de abril de 2015, disponible en: http://bit.ly/2fVBK1q.

[60] *Ibíd.*

(o eximir de cargos por datos) de un grupo definido de sitios o servicios con el fin de aumentar la competitividad respecto de sus competidores.[61] El servicio de música gratuita de T-Mobile es un ejemplo de este tipo de planes de datos "autopatrocinados" por la compañía. Su acuerdo "Music Freedom" les permite a los suscriptores tener acceso a los servicios de *streaming* de música como Pandora, iTunes Radio y Spotify, sin que pese en contra de los límites de uso de datos por parte de los usuarios.[62] En otras palabras, T-Mobile exime del pago por cargos de datos en el uso de su contenido selecto y entonces, "paga" por el *streaming* de música que hacen sus clientes.[63]

Los planes de datos patrocinados son populares entre los proveedores de servicios de telecomunicaciones por una razón. Independientemente de la versión del modelo que adopte la compañía de telecomunicaciones, se beneficia no solo de los pagos recibidos por los proveedores de contenido (salvo que la misma compañía sea la entidad patrocinante), sino además al darles a los usuarios la oportunidad de acceder a datos o servicios gratuitos en la red, lo que lo transforma en algo más atractivo para los suscriptores reales y los potenciales. Los proveedores de contenido, por supuesto, se benefician al aumentar su exposición ante futuros clientes potenciales y al recabar cierta información personal de los usuarios. Los planes de datos patrocinados se asemejan a los planes de sitio único porque en algunos casos incluyen el pago de proveedores de contenido específicos a las compañías de telecomunicaciones para ofrecer su sitio, información o servicios de forma gratuita. Dentro de esta categoría también se pueden incluir los acuerdos en donde Facebook Zero o Google Free Zone pagaron a sus socios de telecomunicaciones para eximir del pago de cargos por datos en el acceso a su contenido o servicios.

Los planes de datos patrocinados han sido criticados por algunas razones. Los defensores de los derechos digitales han condenado al servicio de datos patrocinados de AT&T como una transgresión de los principios de la neutralidad de la red porque trata las distintas fuentes de contenido de manera diferente.[64] Sobre razones puramente económicas y competitivas, los datos patrocinados les "dan ventaja a aquellas compañías con más recursos y (…) capital para invertir en publicidad", mientras deja en desventaja a las empresas que recién se inician y a los empresarios que no pueden pagar a

[61] "Data Caps, Public Knowledge", disponible en: http://bit.ly/2fW6TjL.

[62] Levy, Adam, "T-Mobile Music Freedom Is Ultimately Bad for Consumers", The Motley Fool, 26 de junio de 2014, disponible en: http://bit.ly/2eCl0gz.

[63] *Ibíd*.

[64] Becker, Sam, "Here's Why No One Is Buying into AT&T's Sponsored Data Plan", The CheatSheet, 29 de julio de 2014, disponible en: http://bit.ly/2fJdjp9.

las compañías de telecomunicaciones para que los usuarios tengan acceso a su contenido de forma gratuita.[65] Airtel Zero fue criticada por esas mismas razones.[66] "Music Freedom" de T-Mobile entra en esta categoría también, ya que no admite todos los servicios de *streaming* de música y por ende, puede percibirse como que prioriza ciertas fuentes de contenido (música) en línea en su red a expensas de otras.[67]

Los defensores de los datos patrocinados responden que siempre que el precio del servicio sea razonable con acceso equitativo para todas las compañías que desean participar, no existe discriminación nociva o prejuicio para los clientes, solo beneficios.[68] Desde esta perspectiva, el acceso no discriminatorio para adquirir datos patrocinados no refleja una conducta anticompetitiva o injusta ya que todos son tratados de manera equitativa; este enfoque de "no daño, no perjuicio" lleva a la conclusión de que no habría una violación significativa de la neutralidad de la red bajo esas circunstancias.[69] Los defensores en los Estados Unidos y en India han relacionado los planes de datos patrocinados con el servicio "de llamada gratuita" o el "1-800" aprobado por la Comisión Federal de Comunicaciones, donde las compañías son las que sirven al interés público mediante el pago de cargos en lugar de los consumidores.[70]

I.A.III. *Zero-rating* compuesto

Los planes zero-rating compuesto son aquellos donde una compañía (o compañías) patrocinante se asocia con un proveedor de servicios de telecomunicaciones para brindarles a los suscriptores acceso a una gran cantidad

[65] *Ibíd*.

[66] "CEO Defends Airtel Zero", *supra* nota59.

[67] *Véase*, por ejemplo, Masnick, Mike, "Music Freedom or Holding Consumers Hostage? Letting ISPs Pick Winners and Losers Is a Problem", Techdirt, 19 de junio de 2014, disponible en: http://bit.ly/1nRmbUE.

[68] *Véase*, por ejemplo, "Airtel Launches 'Airtel Zero': A Win-Win Platform for Customers and Marketers", Airtel, 6 de abril de 2015, disponible en: http://bit.ly/2gYOV37; Anderson, Steve, "Airtel Unveils Sponsored Data Services", Next Generation Digital Services, 7 de abril de 2015, disponible en: http://bit.ly/2fUPV7H.

[69] "CEO Defends Airtel Zero", *supra* nota59.

[70] *Véase*, "AT&T Introduces Sponsored Data for Mobile Data Subscribers and Business", AT&T, 6 de enero de 2014, disponible en: http://soc.att.com/2fRUzRm; Bode, Karl, "Despite Limited Interest in AT&T's Sponsored Data, Company Still 'Bullish' on its Awful Precedent", Wireless, 5 de febrero de 2015, disponible en: http://bit.ly/2ge51Wo ("Escuchar a AT&T decirlo en ese momento, sería similar a 'envío sin costo' o un número gratuito de 0-800 para datos…"); "CEO Defends Airtel Zero", *supra* nota59.

de sitios y servicios selectos. En general, estas plataformas de zero-rating brindan acceso libre a una gran variedad de contenido local selecto o de otra naturaleza, según lo determine la compañía patrocinante, siempre con el asesoramiento de las autoridades gubernamentales.[71] Por consiguiente, estos planes son similares a una plataforma de ofertas cuidadosamente seleccionadas a la que se accede a través del teléfono móvil del suscriptor. A diferencia de los servicios de datos patrocinados, no requieren de pagos a o por parte de las compañías de telecomunicaciones que pueden renunciar a dichas tarifas a cambio de ofertas mejoradas a los clientes y una base de suscriptores más grande.[72] Las compañías de telecomunicaciones se benefician cuando atraen a nuevos usuarios que, de otro modo, no serían capaces de (o no querrían) pagar por un plan de datos y por acceso en línea. Los proveedores de contenido y las compañías de telecomunicaciones pueden argumentar que ofrecen un servicio y, al mismo tiempo, crean oportunidades de mercado para que los usuarios puedan acceder a datos o servicios adicionales por una tarifa.[73] A pesar de su uso aparente, estos planes están entre el tipo de zero-rating más polémico de la actualidad, por una serie de razones que se debaten a continuación.

Tal como se mencionó antes, Google Free Zone goza de atributos tanto de los planes de *zero-rating* de servicio único como de *zero-rating* compuesto.[74] Airtel Zero, en India, combinó características de datos patrocinados y de *zero-rating* compuesto antes de cerrar debido a la decisión emitida por el ente regulador de India donde se estipula la prohibición de toda tarifa diferencial por parte de las compañías de telecomunicaciones, incluso el

[71] "Mark Zuckerberg y el presidente de Colombia, Juan Manuel Santos, lanzan Internet.org en Bogotá" ("Internet.org App Launches in Colombia"), Internet.org, 14 de enero de 2015, disponible en: http://bit.ly/2gMkytN; *Véase además*, Antunes, Anderson, "*Mark Zuckerberg Meets with Brazil's President at the 7th Summit of the Americas, in Panama*", *Forbes*, 11 de abril de 2015, disponible en: http://bit.ly/2fJeipn; Constine, Josh, "Indian Prime Minister Tells Zuckerberg Social Media Creates a New Form of Diplomacy", Techcrunch, 27 de septiembre de 2015, disponible en: http://tcrn.ch/2gYM76l.

[72] Post, David, "Facebook, Internet.org, and the Net Neutrality Bugaboo", *Washington Post*, 17 de agosto de 2015, disponible en: http://wapo.st/2gbRevD.

[73] Existe evidencia de que este modelo de negocios funciona. Facebook informa que "más de la mitad de las personas que están en línea a través de Internet.org pagan por los datos y para acceder a internet dentro de los primeros 30 días". "One Year in: Internet.org Free Basic Services", Internet.org, 27 de julio de 2015, disponible en: http://bit.ly/2gcQRFz; *Véase además*, Peel, Anna, "Facebook: More People Are Online Thanks to Internet.org", Value Walk, 27 de julio de 2015, disponible en: http://bit.ly/2gKaXWJ (cita al VP de Facebook, Chris Daniels, cuando dice que los usuarios que se unen a Internet.org posteriormente "desean seguir y experimentar más en la internet").

[74] Véase, *supra* notas 37-42 y texto acompañante.

zero-rating.[75] El sitio Internet.org original de Facebook, que ahora es parte de la plataforma de conectividad de Free Basics, es un ejemplo genuino de un plan de *zero-rating* compuesto.[76]

Fundada en agosto 2013, Internet.org pretende cerrar la brecha digital brindando acceso sin cargo a decenas de servicios en internet a poblaciones enteras en los países menos desarrollados, y, por una tarifa, un acceso más amplio.[77] Es una "iniciativa que reúne a líderes tecnológicos, comunidades locales y compañías sin fines de lucro con el fin de conectar a los dos tercios [sic] del mundo que no tiene acceso a internet".[78] Por ejemplo, entre los sitios y servicios gratuitos que Internet.org ofrecía en India antes de cerrar se pueden nombrar a Facebook, Messenger, BBC World News, Bing Search, y Wikipedia. Asimismo, ofrecía acceso a sitios locales que brindan información sobre clima, deportes, anuncios clasificados de empleos, información sobre salud, cuidado infantil y maternal e incluso música, todo a nivel local.[79] En cuanto a este emprendimiento, a la fecha Facebook se ha asociado con Airtel, Ericsson y Nokia, entre otros.[80] En la actualidad, Internet.org alcanza a más de mil millones de personas en, al menos, 42 naciones en África, Asia

[75] Véase, *supra* notas 59-61 y texto acompañante; Press Release No. 13/2016, Telecom Regulatory Authority of India, 8 de febrero de 2016, disponible en: http://bit.ly/1Q4SElh.

[76] Constine, Josh, "Internet.Org's App with Free Access to Facebook, Google, Wikipedia, Local Info Launches in Zambia", Tech Crunch, 31 de julio de 2014, disponible en: http://tcrn.ch/1odKN6N; Mirani, Leo, "Millions of Facebook Users Have No Idea They're Using the Internet", Quartz, 9 de febrero de 2015, disponible en: http://bit.ly/2fJmna6; "Update to Internet.org Free Basic Services", Internet.org, 24 de septiembre de 2015, disponible en: http://bit.ly/2g11MRs.

[77] "Who We Are", Internet.org, disponible en: http://bit.ly/151flSx.

[78] *Ibíd*.

[79] Alwani, Rishi, "Facebook's Internet.org Comes to India: Everything You Need to Know", NDTV Gadgets, 11 de febrero de 2015, disponible en: http://bit.ly/2g10tCe; *Véase además*, "Internet.org App Now Available in India", Internet.org, 10 de febrero de 2015, disponible en: http://bit.ly/2fZR6yQ. Internet.org no ofrece a los usuarios acceso a un servicio de correo electrónico. Las ofertas de Internet.org varían según el país, y en la mayoría de los casos no son tan amplias como las disponibles en India. Este es el caso, por ejemplo, en Zambia y Colombia. Rosen, Guy, "Introducing the Internet.org App", Internet.org, 31 de julio de 2014, disponible en: http://bit.ly/2gbQ6lm; "Internet.org App Launches in Colombia", Internet.org, 14 de enero de 2015, disponible en: http://bit.ly/2gCSUPs.

[80] *Véase*, Lunden, Ingrid, "Facebook-Led Internet.org Partners with Nokia on SocialEDU in Rwanda, Unilever in India, Ericsson on New Lab to Connect Developing Economies", TechCrunch, 24 de febrero de 2014, disponible en: http://tcrn.ch/2fPmsl5. Disponible en: http://tcrn.ch/2gPvaqM.

y América Latina.[81] Esos países incluyen Bangladesh, Colombia, Ghana, India, Indonesia, Kenia, México, Nigeria, Pakistán, las Filipinas, Senegal, Sudáfrica, y Zambia.[82]

La misión declarada de Facebook para la plataforma Internet.org/Free Basics es llevar conectividad a aquella parte de la población mundial que aún no la tiene.[83] Muchos cuestionan la justificación altruista para esta iniciativa, y sostienen que en el fondo se trata de una táctica de expansión comercial.[84] Por ejemplo, la implementación de Internet.org en India en febrero de 2015 desató una ola de protestas por parte de activistas de derechos digitales en todo el mundo, preocupados por la protección de la neutralidad de la red, la libertad de expresión y la privacidad.[85] En una respuesta coordinada a la defensa pública de Internet.org por parte de Mark Zuckerberg,[86] decenas de grupos defensores a nivel nacional e internacional, entre ellos Access, Bits of Freedom y el Center for Media Justice opinaron sobre el concepto de la neutralidad de la red de Facebook y sostuvieron que no se basa en una definición "verdadera" de ese término.[87] Expresaron su preocupación por el hecho de que "el acceso para los más pobres [se estaba] construyendo como una justificación por las violaciones a la neutralidad de la red".[88] Desde su perspectiva, debido a que el *zero-rating* que es la base de Internet.org es "discriminatoria por naturaleza", no solo viola la neutralidad de la red, sino que además:

> Pone en peligro la libertad de expresión y la igualdad de oportunidades al permitir que los proveedores de servicios decidan qué servicios de internet tendrán privilegios por sobre otros, de esa manera interfieren con el libre flujo de información y con el derecho de las personas en relación con las redes.[89]

---

[81] *Véase*, Sirohi, Seema, "Sorry Mark Zuckerberg, the World Bank Also Disagrees with You", *The Economic Times: Letter from Washington*, 16 de enero de 2016, disponible en: http://bit.ly/2fl6gik

[82] "Where We've Launched", Internet.org, disponible en: http://bit.ly/2g16vTd

[83] *Véase*, *ibíd*.; "Announcing the Internet.org Platform", Facebook Newsroom, 4 de mayo de 2015, disponible en: http://bit.ly/2fJkJJ4

[84] Véase, por ejemplo, Imtiaz Asif, "Nothing Altruistic About Facebook's Initiative to Spread the Internet", *US Finance Post*, 6 de enero de 2014, disponible en: http://bit.ly/2fl66rg; K.J., Shashidhar, "Sunil Mittal Calls It Right: What Zuck Is Doing with Internet.org Isn't Philanthropy", Medianama, 9 de marzo de 2015, disponible en: http://bit.ly/2gMg06X.

[85] *Véase*, *supra* notas 4, 5 y 15, y texto acompañante.

[86] *Véase*, *supra* nota 17 y texto acompañante.

[87] Carta abierta, *supra* nota8.

[88] *Ibíd*.

[89] *Ibíd*.

Frente a la crítica de que actuaba como "guardia" cuando seleccionaba aplicaciones, servicios y contenido, creando así una internet de "dos niveles" para los usuarios, Facebook anunció, en mayo de 2015, que abría su plataforma Internet.org en términos generales a "todo servicio en línea con ancho de banda reducido que cumpliera con las pautas técnicas".[90]

I.A.IV. *Zero-rating* falso (o no selectivo)

Los planes de *zero-rating* falso son aquellos que parecen involucrar la neutralidad de la red pero, en efecto, no lo hacen. En este modelo, un proveedor de contenido se asocia con una o más compañías de telecomunicaciones para ofrecer una cantidad limitada de datos gratuitos a los usuarios a cambio de ciertas condiciones, como mirar un anuncio o descargar una aplicación. Los usuarios pueden elegir si usan los datos complementarios. Debido a que ni los proveedores de contenido ni las compañías de telecomunicaciones deciden a qué aplicaciones, servicios o sitios accede el suscriptor con su asignación de datos gratuitos, los planes de *zero-rating* falso no generan cuestiones sobre la discriminación o la no competitividad de la neutralidad de la red, como sí lo hacen las prácticas de *zero-rating* "selectas" o "verdaderas".[91] En términos estrictos, esos planes no son *zero-rating* para nada, según la definición de *zero-rating* como práctica que limita la selección del cliente en su acceso a internet móvil, como sucede comúnmente.[92] Las compañías de telecomunicaciones y los proveedores de internet se benefician de los planes de *zero-rating* falso al atraer a nuevos clientes hacia sus marcas, o hacia sus programas o equipos específicos, si bien las compañías de telecomunicaciones también se benefician al ofrecerles a los clientes la oportunidad de mejorar su acceso a los datos, sin atentar contra la neutralidad de la red.

Las estrategias de Mozilla llamadas de "tasa equitativa" que apuntaban a expandir los mercados mientras contribuían a cerrar la brecha digital en el mundo en vías de desarrollo son el ejemplo perfecto.[93] Según el punto de

[90] Ribeiro, John, "Facebook's Internet.org Opens Platform to Other Online Services", Computerworld, 4 de mayo de 2015, disponible en: http://bit.ly/2eXwrOx.

[91] *Véase*, Bode, Karl, "Mozilla: If Facebook Really Wants to Help Developing Nations,it Should Ignore Zero Rating and Fund Real internet Access", Techdirt, 15 de mayo de 2015, disponible en: http://bit.ly/1lFSmmx.

[92] Véase, *supra* nota 8 y texto acompañante; Baker, Mitchell, "Zero Rating and the Open Internet", Lizard Wrangling: Mitchell on Mozilla & More, 6 de mayo de 2015, disponible en: http://bit.ly/2gpRcDD ("*Zero-rating* en su práctica actual es un *zero-rating* selecto para unas pocas aplicaciones y sitios web; con exclusión del resto de internet").

[93] Baker, *supra* nota92.

vista de Mozilla, las prácticas predominantes de *zero-rating* "selectivo" son la respuesta incorrecta a la pregunta correcta que plantea cómo promover una mayor conectividad en el mundo en vías de desarrollo:

> La respuesta correcta es que todos los datos se transmiten por un mismo precio, ya sea "cero" u otro precio. De esta forma, los clientes eligen a qué contenido quieren acceder según la calidad del mismo y no según el poder financiero ni las sociedades comerciales del proveedor. Así, los nuevos empresarios pueden alcanzar a todos los usuarios de internet, incluso si se tratara de unas pocas personas trabajando en un espacio laboral compartido sin posibilidad de subsidiar cargos por datos.[94]

En aras de estas estrategias, Mozilla anunció en mayo de 2015 su asociación con Orange, un proveedor de servicios de telecomunicaciones a escala global que opera en diversos países de África y de Oriente Medio, para ofrecer un teléfono Orange a bajo costo que utiliza el sistema operativo Firefox en 13 mercados nuevos.[95] El teléfono Klif, como se lo denomina, cuesta aproximadamente 40 dólares estadounidenses e incluye tiempo ilimitado de llamadas y 500 MB de datos libres por mes durante seis meses.[96] Esta iniciativa supuestamente se basó en la experiencia de Mozilla en Bangladesh, donde se asoció con Grameenphone (compañía de Telenor) con el fin de ofrecer a sus usuarios 20 MB de datos libres por día en internet si el cliente primero mira un anuncio publicitario.[97] Según la visión de Mozilla, "este tipo de acuerdos podrían representar una solución a largo plazo para los problemas clave subyacentes de la inclusión y la igualdad digital", sin las consecuencias negativas causadas por las prácticas de *zero-rating* selectivo.[98]

Mozilla no es la única compañía innovadora en esta área. Desde 2014, Jana, una compañía radicada en Boston, promueve la aplicación mCent, con muy buena repercusión.[99] La aplicación alienta a los usuarios a acceder a

---

[94] *Ibíd*.

[95] Dixon-Thayer, Denelle, "Mozilla View on Zero-Rating", Mozilla, 5 de mayo de 2015, disponible en: https://mzl.la/2gYRjqB "Firefox OS Proves Flexibility of Web", Mozilla, 1 de marzo de 2015, disponible en: https://mzl.la/2fVFNL0. Los países en donde se ofrecerá, en primera instancia, el teléfono Klif incluyen Egipto, Senegal, Túnez, Camerún, Botsuana, Madagascar, Mali, Costa de Marfil, Jordania, Níger, Kenia, Mauricio y Vanuatu.

[96] Dixon-Thayer, *supra* nota95.

[97] *Ibíd*.

[98] *Ibíd*.

[99] *Véase*, Olson, Parmy, "This App Is Cashing in on Giving the World Free Data", *Forbes*, 29 de julio de 2015, disponible en: http://bit.ly/2fVFYpE.

sitios o servicios de terceros en forma gratuita mediante la acreditación de sus planes de datos.[100] Entonces, "se les otorga tiempo de aire a los usuarios para una serie de distintos tipos de actividades, incluso para descargar y usar aplicaciones, contestar encuestas, ver videos, suscribirse a servicios o participar de concursos".[101] Los proveedores de contenido que se asocian a mCent, como Twitter y Amazon, así como otros servicios de mensajería y música locales, le pagan a Jana para que sus aplicaciones estén disponibles a los suscriptores y así probarlas a través de mCent.[102] Se espera que supere los 30 millones de usuarios en los países en vías de desarrollo.[103]

Asimismo, el nuevo emprendimiento Marvin en India y en Silicon Valley emplea una estrategia para recompensar a los clientes con datos gratuitos cuando acceden al contenido en línea a través de la aplicación de Marvin, Gigato. Como ocurre con mCent, Gigato combina aspectos de datos patrocinados y *zero-rating* falso.[104] Los clientes corporativos pagan para que sus servicios y sitios se publiciten en los teléfonos de los usuarios a través de contenido y anuncios estratégicamente ubicados.[105] Cuando los consumidores acceden a sitios de terceros, Gigato acredita el plan de datos de los usuarios en forma directa.[106] El suscriptor puede usar los créditos de datos para acceder a cualquier contenido de internet que elija. Según se publicó: "Gigato brinda datos de internet en forma gratuita y sin límite para su Android. Utilice las aplicaciones que desee y obtenga megabytes para su cuenta prepaga".[107]

I.B. Perspectivas nacionales sobre acceso a internet y neutralidad de la red

En esta sección, centramos nuestra atención al escenario regional y nacional en donde se implementan las políticas de neutralidad de la red, como el *zero-rating*. Se divide en tres subsecciones. La primera se centra en ordenar indicadores estadísticos clave para una muestra de diez países organizados por

[100] *Véase*, Informe Public Knowledge de Rossini y Moore, *supra* nota24, en 7.

[101] "About Us", mCent, 2015, disponible en: http://bit.ly/2fIfATb.

[102] *Véase*, Olson, *supra* nota99.

[103] *Véase*, Howard, Alexander, "Gigato Tried to Make Internet Access Affordable with Data Rebates", Huffington Post, 31 de julio de 2015, disponible en: http://huff.to/2gMpHCe.

[104] *Ibíd.*

[105] *Véase*, Informe Public Knowledge de Rossini y Moore, *supra* nota 24; *véase además*, "Surf More. Save More", Gigato, disponible en: http://bit.ly/2gkMVlF.

[106] Informe Public Knowledge de Rossini y Moore, *supra* nota 24.

[107] Gigato Application, Google Play, 29 de septiembre de 2015, disponible en: http://bit.ly/1SFxtZ9.

región (África, Asia, Europa y América del Norte y América del Sur). Fueron seleccionados mediante criterios que apuntan a combinar una diversidad funcional de experiencias globales observadas desde una perspectiva cuantitativa y cualitativa. Los criterios aplicados incluyeron la representación regional; la política o la práctica relacionada con la neutralidad de la red y el *zero-rating*; el estado de país desarrollado, país en vías de desarrollo o menos desarrollado[108]; y los niveles de libertad democrática y de internet. Los indicadores cuantitativos seleccionados proporcionan una muestra representativa de cada país en cuanto a su situación de desarrollo social, económico y político, e incluye cifras para la cobertura de internet móvil y fija. En su conjunto, estos datos presentan un panorama general pero útil sobre los diferentes escenarios locales en donde existe el *zero-rating* en todo el mundo. La segunda subsección da un giro hacia a una perspectiva temática, observa las diferentes barreras al acceso a internet, tal como se manifiestan en los países con baja conectividad. La última sección pretende llegar a un entendimiento mucho más profundo de cómo abordan la cuestión del *zero-rating* los gobiernos en distintos contextos internos, a través del estudio de casos en tres países.

I.B.I. Antecedentes y contexto

En la actualidad hay al menos 60 Estados que autorizan, de manera activa, alguna forma de *zero-rating* en la práctica.[109] Pero hay cada vez más países que han prohibido esa práctica o que están a punto de hacerlo. De manera considerable, el Consejo de Europa adoptó recientemente las pautas sobre

[108] Para una descripción más detallada de la tipología de desarrollo del país utilizada en este artículo, véase, *infra* la tabla 3, *infra* notas 126-128; *Véase además*, "La División de Estadística de las Naciones Unidas. Composición de las regiones, países o zonas clasificados por grupos económicos, comerciales y de otro tipo", 31 de octubre de 2013, disponible en: http://bit.ly/2bQCsNZ.

[109] *Véase*, Wikipedia Zero, supra nota 34; Wikipedia, Internet.org, disponible en: http://bit.ly/2gbWdMQ (Colombia, Ghana, Guatemala, India, Kenia, Filipinas, Tanzania, y Zambia); "Are You in the Zone?", Google Free Zone, disponible en: http://bit.ly/2gkV8pT (India, Nigeria, Filipinas, Sri Lanka, y Tailandia); Mims, Christopher, "Facebook's Plan to Find Its Next Billion Users: Convince Them the Internet and Facebook Are the Same", Quartz, 24 de septiembre de 2012, disponible en: http://bit.ly/2gPp35w (Argentina, México); Rewheel, Antonios Drossos, "Forget Fast Lanes. The Real Threat for Net-Neutrality Is Zero-Rated Content", Gigaom, 26 de abril de 2014, disponible en: http://bit.ly/2fRpJlA (Estados Unidos); Wikipedia, Facebook Zero, disponible en: http://en.wikipedia.org/wiki/Facebook_Zero (Bangladesh, Camerún, El Salvador, Fiji, Francia, Alemania, Grecia, Georgia, Guinea, Indonesia, Kosovo, Malasia, Marruecos, Birmania, Nueva Zelanda, Pakistán, Panamá, Filipinas, Polonia, Catar, Surinam, Trinidad y Tobago, Túnez, Reino Unido, Zimbabue).

la neutralidad de la red que podrían restringir el uso del *zero-rating* en toda Europa,[110] si bien la implementación efectiva de esas salvaguardas por los Estados miembro sigue siendo una preocupación.[111] Asimismo, los siguientes países tienen o han tenido leyes que no permiten o expresamente prohíben las prácticas de *zero-rating*: Chile, Brasil, Noruega, Holanda, Finlandia, Islandia, India, Estonia, Letonia, Lituania, Malta, Japón, y Eslovenia.[112] Varios países que en el pasado tan solo desalentaban la práctica de *zero-rating*, la prohíben en el presente.[113] De manera sorprendente, ninguno de los países que prohíbe en la actualidad el *zero-rating* está en África. Chile, Brasil y ahora India son las únicas naciones en vías de desarrollo que prohíben el *zero-rating* en la actualidad, si bien la aplicación de las regulaciones es permisiva y la práctica continúa.[114] Con el propósito de entender mejor los perfiles de cada país –aquellos que permiten el *zero-rating* y aquellos que no lo hacen– la presente subsección compila los indicadores clave que miden las condiciones sociales, económicas y políticas en una muestra representativa de diez países en las principales regiones del mundo. Organiza los datos en

[110] McCarthy, Kieran, "Council of Europe Gets Tough on Net Neutrality", *The Register*, 13 de enero de 2016, disponible en: http://bit.ly/2gPqDEA ("Las pautas no son legalmente vinculantes pero es muy probable que deriven en legislación que siga su camino y sea aprobada en Europa. El consejo está separado de la Unión Europea pero tiene influencia ya que está formado por ministros extranjeros y otros políticos de 47 Estados miembro").

[111] Carta abierta de Sir Tim Berners-Lee, el profesor Lawrence Lessig, y la profesora Barbara van Schewick, "We Have Four Days to Save the Open internet in Europe", Web Foundation, 14 de julio de 2016 (de aquí en adelante la Carta abierta); Bode, Kari, "Europe's Flimsy Net Neutrality Rules Go Live, Are Actually Worse than No Rules At All", TechDirt, 6 de mayo de 2016, disponible en: http://bit.ly/2fJGLaY.

[112] Los Estados que la prohibieron antes que lo hiciera India eligieron hacerlo en febrero de 2016: Chile, Brasil, Noruega, Holanda, Finlandia, Islandia, Estonia, Letonia, Lituania, Malta, Japón y Eslovenia. *Véase*, Guha, Romit, y Aulakh, Gulveen, "Zero Rating: What Are Countries Doing About It", *The Times of India*, 21 de abril de 2015, disponible en: http://bit.ly/2gMlyOC; Layton y Elaluf-Calderwood, *supra* nota24; *Véase, además*, Informe Public Knowledge de Rossini y Moore, *supra* nota 24, en 39 (se descubrió que las protecciones sobre neutralidad de la red recientemente sancionadas en Brasil no permiten excepciones al *zero-rating*).

[113] Para aquellos estados que desalientan el *zero-rating* y donde las compañías de servicios inalámbricos no utilizan dicha práctica; *Véase*, Meyer, David, "Pro-net Neutrality Norway Advises Carriers to Avoid Zero-Rating", Gigaom, 18 de noviembre de 2014, disponible en: http://bit.ly/2gMlxtW (Noruega, Finlandia, Suecia, Estonia, Lituania, Letonia, Malta, e Islandia - de estos países todos menos Suecia ahora tienen leyes contra el *zero-rating*).

[114] *Véase*, "Country Classifications by Region and Development Status", International Telecommunication Union, disponible en: http://bit.ly/2fJep4r. Véase, División de Estadísticas de la ONU, *supra* nota 108; Informe Public Knowledge de Rossini y Moore, *supra* nota 24, en 16-20 (Chile); 39-46 (Brasil). Para un debate sobre la situación actual en India, véase, *infra* Parte III.B.

una serie de tablas ilustrativas, donde cada una destaca factores fundamentales en el análisis a seguir en las partes subsiguientes de este artículo, tal como se explica más adelante.

La tabla 1 resume, de manera general, la condición actual en los países seleccionados, respecto de los esfuerzos que realizan para regular la neutralidad de la red y el *zero-rating*, organizada por región, a saber:

Tabla 1. Contexto de la neutralidad de la red y *zero-rating* por región

País	Región	Neutralidad de la red	*Zero-rating*
Sudáfrica	**África**	No regulada	Permitida
Zambia		No regulada	Permitida
India	**Asia**	No regulada	Prohibida
Malasia		No regulada	Permitida
Holanda	**Europa**	Regulada por ley[115]	Prohibida
Eslovenia		Regulada por ley[116]	Prohibida
Canadá	**América del Norte**	Regulada por agencia administrativa[117]	Prohibida
Estados Unidos		Regulada por agencia administrativa[118]	Permitida en ciertos casos
Chile	**América del Sur**	Regulada por ley[119]	Prohibida*
Colombia		Regulada por ley[120]	Permitida

La tabla 2 presenta datos sobre el acceso a internet con banda ancha fija y móvil para los mismos países. Las estadísticas están ordenadas de manera tal que resaltan el porcentaje de suscripciones a la banda ancha fija en cada país, en forma descendente desde el nivel más bajo hasta el más elevado de penetración.

[115] *Infra* Parte I.B.II.e.

[116] Wieland, Ken, "Mobile Operators in Slovenia Fall Foul of Net Neutrality Rules", Mobile World Live, 26 de enero de 2015, disponible en: http://bit.ly/2fAEykL

[117] Gobierno de Canadá, Comunicado de prensa, archivado, "CRTC Continues to Set the Course for the Future of Television with Let's Talk TV Decisions", 29 de enero de 2015, disponible en: http://bit.ly/2fJFilb

[118] *Infra* Parte I.B.II.g.

[119] *Infra* Parte I.B.II.a. *El *zero-rating* está prohibido por ley pero, en la práctica, es tolerado.

[120] *Infra* Parte I.B.II.b.

Tabla 2. Acceso a internet con banda ancha fija y móvil

País	Región	Suscripciones a banda ancha fija en el 2014 (cada 100 personas)[121]	Suscripciones a banda ancha móvil en el 2013 (cada 100 personas)[122]	Suscripciones a celulares/ móviles en el 2014 (cada 100 personas)[123]	Usuarios de internet en el 2014 (cada 100 personas)[124]
Zambia	África	0,14	0,7	67	17,3
India	Asia	1,24	3,2	74	18,0
Sudáfrica	África	3,21	25,2	150	49,0
Malasia	Asia	10,14	12,5	149	67,5
Colombia	América del Sur	10,27	7,9	113	52,6
Chile	América del Sur	14,08	35,6	133	72,4
Eslovenia	Europa	26,55	41,8	112	71,6
Estados Unidos	América del Norte	30,37	92,8	98	87,4
Canadá	Sin datos	34,38**	41,0	83	87,1
Holanda	Sin datos	41,02	62,3	116	93,2

** Los datos sobre acceso a la banda ancha fija en Canadá de 2014 no estaban disponibles, por lo que se utilizaron los datos de 2013.

Se comparan las estadísticas de acceso a la banda ancha fija con aquellas que muestran la cobertura de telefonía móvil y las suscripciones al servicio de banda ancha inalámbrica. Los países de Europa y de América del Norte tienen una penetración de banda ancha fija mucho mayor al de otras regiones (Corea del Sur y Japón son las excepciones en Asia). Pero los datos de la cobertura del servicio celular móvil son bastantes similares en todas las regiones, con niveles especialmente elevados (más del 100%) en algunas naciones de Asia, África y América del Sur. Cabe destacar que Sudáfrica cuenta con la cobertura móvil más elevada entre los diez países estudiados, pero tiene el tercer porcentaje más bajo en cuanto a penetración de banda ancha fija. Asimismo, es importante destacar la diferencia entre

[121] "Suscripciones a banda ancha fija (cada 100 personas)", Banco Mundial, disponible en: http://bit.ly/1VWgtnl.

[122] "Perfil de país", ITU, disponible en: http://bit.ly/1Pk9X5l.

[123] "Suscripciones a celulares/móviles (cada 100 personas)", Banco Mundial, disponible en: http://bit.ly/1K1NbPY. Las suscripciones celulares móviles se definen como aquellas que brindan acceso a comunicación de voz al servicio público de telefonía móvil que usan tecnología celular.

[124] "Usuarios de internet (cada 100 personas)", Banco Mundial, disponible en: http://bit.ly/1hq7God. Los usuarios de internet se definen como aquellas personas que tienen acceso a la red global.

el acceso de banda ancha móvil, que aún es relativamente escaso en los países en vías de desarrollo, y el acceso a servicio celular móvil en esos mismos países, que como ya se señaló, puede ser muy elevado y estar a la altura de sus pares más desarrollados en Europa y América del Norte. Es importante recordar aquí que el acceso a los planes de *zero-rating,* descriptos en la primera sección, es a través de teléfonos celulares (no teléfonos inteligentes) y no requiere cobertura de banda ancha.

La tabla 3 muestra el producto bruto interno (PBI) per cápita de cada país en orden ascendente desde el más bajo al más alto. Compara el PBI de cada país con su nivel de desarrollo y desigualdad según los datos del Programa de las Naciones Unidas para el Desarrollo (PNUD). Al analizar las tablas 2 y 3, se observa –de manera poco sorprendente– que el PBI per cápita se correlaciona considerablemente con el uso general de internet, y en especial, en lo que refiere a la penetración de banda ancha fija. Resulta interesante el hecho de que la cobertura móvil, y a un menor grado, la penetración de banda ancha móvil muestra una baja correlación con el PBI per cápita o la desigualdad de ingresos. Por ejemplo, Chile posee la penetración de banda ancha móvil más alta entre los países estudiados fuera de Europa y América del Norte, a pesar de tener un PBI per cápita mediano y clasificar en tercer lugar en términos de desigualdad de ingresos del grupo.

Tabla 3. PBI y Estadísticas sobre índices de desarrollo humano

País	Tasa de alfabetismo en adultos (porcentaje)[125]	PBI per cápita[126] en 2014	Índice de GINI sobre desigualdad[127] (0 es "igualdad perfecta", 100 es "desigualdad perfecta")	Clasificación del índice de Desarrollo Humano del PNUD en 2014 (de 187 países) y posición de alcance)[128]
Zambia	84	4086,00	55,6	141 (medio)
India	69	5.833,30	33,9	135 (medio)
Sudáfrica	93	3.046,20	63,4	118 (medio)
Colombia	94	13.046,40	53,5	98 (elevado)
Chile	97	22.333,10	50,5	41 (muy elevado)
Malasia	Sin datos	24.714,80	46,3	62 (elevado)
Eslovenia	100	29.917,00	25,6	25 (muy elevado)
Canadá	Sin datos	44.088,50	33,7	8 (muy elevado)
Holanda	Sin datos	47.130,70	28,0	4 (muy elevado)
Estados Unidos	Sin datos	54.629,50	41,1	5 (muy elevado)

Por último, la tabla 4 analiza varios indicadores que reflejan los niveles de democracia y de libertad política, de corrupción y de libertad en internet de cada país. En términos generales, los países de Europa y de América del Norte muestran tendencias más fuertes en estas áreas comparados con la mayoría de los países de otras regiones. Cabe destacar que los países incluidos en nuestro estudio que han prohibido el *zero-rating* poseen los niveles de democracia más altos (9 ó 10 de 10). Asimismo, la mayoría de los países que prohíben el *zero-rating* alcanzan un buen puntaje en el índice de percepción de la corrupción, con excepción de India y posiblemente, Eslovenia.

[125] "Tasa de alfabetismo en adultos, Población de más de 15 años, ambos sexos (%)", Banco Mundial, disponible en: http://bit.ly/1BUA0pA (refleja las estadísticas más recientes publicadas por el Banco Mundial: 2009-2013).

[126] "PBI per cápita, PPP ($ internacional actual)", Banco Mundial, disponible en: http://bit.ly/18gtvTm. Según el Banco Mundial, "el PBI según la paridad del poder adquisitivo es el producto bruto interno convertido a dólares internacionales mediante los índices de paridad del poder adquisitivo. El dólar internacional tiene el mismo poder adquisitivo sobre el PBI que el que posee el dólar estadounidense en los Estados Unidos".

[127] "Índice GINI", Banco Mundial, disponible en: http://bit.ly/TLu3fJ (refleja los datos estadísticos más recientes publicados por el Banco Mundial: 2009-2013).

[128] Tablas estadísticas de desarrollo humano, tabla 1, Programa de Desarrollo de las Naciones Unidas, disponible en: http://bit.ly/1kYwvXA.

Tabla 4. Índices de democracia, libertad y corrupción

País	Índice Freedom House de 2015 (1 es "el más libre"; 7 "el menos libre")[129]	Puntaje sobre libertad de internet de Freedom House de 2015 (0 es el mejor, 100 es el peor)[130]	Índice sobre Democracia Polity IV de 2014 (de un total de 10)[131]	Índice de percepción de la corrupción[132] de 2014 (0 es "altamente corrupto"; 100 es "muy transparente")
Malasia	4	"Libre parcialmente" - 43	6	52
Colombia	3,5	"Libre" - 32	7	37
Zambia	3,5	"Libre parcialmente" - 40	7	38
India	2.5	"Libre parcialmente" - 40	9	38
Sudáfrica	2	"Libre" - 27	9	44
Eslovenia	1	Sin datos	10	58
Chile	1	Sin datos	10	73
Estados Unidos	1	"Libre" - 19	10	74
Canadá	1	"Libre" - 16	10	81
Holanda	1	Sin datos	10	83

I.B.II. Barreras a la conectividad

Nadie cuestiona la continuidad de la gran brecha entre la población mundial que goza de acceso a la conexión a internet y la otra parte que no lo hace, así como tampoco el hecho de que la mayor parte de esa población que goza de derechos digitales vive en los países desarrollados. La cantidad total de usuarios de internet ha crecido rápidamente durante las últimas dos décadas a más de 3 mil millones, en la actualidad, de los cuales casi el 80% vive en países desarrollados.[133] "Los países en vías de desarrollo [por otro lado] albergan casi el 90% de los 4 mil millones de personas que aún

[129] "Freedom in the World 2015", Freedom House, 2015, disponible en: http://bit.ly/2fCTl8Y.

[130] "2015 Freedom on the Net", Freedom House, 2015, disponible en: http://bit.ly/1M1okue.

[131] "Polity IV Annual Time Series, 1800-2013", Integrated Network for Societal Conflict Research, 2013, disponible en: http://bit.ly/2fPqbWc.

[132] "2014 Índice de percepción de la corrupción", Transparency International, 2014, disponible en: http://bit.ly/1tLovwg.

[133] *Ibíd*.

no usan internet".[134] Entonces, por ejemplo, "mientras en Europa la tasa de penetración de internet supera el 75%, en África solamente alrededor del [20%] de los hogares están conectados".[135] Esto ocurre en otros lugares también: India e Indonesia, dos de las naciones más pobladas del mundo, tienen tasas de usuarios de internet por debajo del 20%.[136] Estas estadísticas revelan no solo la existencia de una brecha digital *entre* Estados sino también *dentro* de ellos. Las condiciones técnicas, políticas, sociales y económicas de la brecha digital *a nivel mundial* conforman una mera aglutinación de las causas detrás de la brecha digital *a nivel local* que separa a los que "tienen" de los que "no tienen", en lo que respecta al acceso digital, dentro de una sociedad particular. No debe sorprender, entonces, que quienes se encuentran en la línea de frente en la lucha para cerrar esa brecha, son justamente los países en vías de desarrollo, que cuentan con la proporción más grande de personas sin derechos digitales, y no poseen los grandes beneficios sociales, económicos, políticos y culturales ofrecidos por la conexión a internet.[137]

En términos generales, las barreras de la conectividad predominantes en la mayoría de los países en vías de desarrollo entran en dos categorías: "rígidas" y "flexibles". Las barreras rígidas comprenden aquellos factores externos que determinan si existe un acceso técnico a la conexión a internet o si puede implementarse en una sociedad particular. Entre esos factores podemos nombrar la falta de infraestructura física, la calidad de las conexiones a internet donde las hubiera y el costo elevado de acceso en los países con bajos ingresos.[138] Por otro lado, las barreras flexibles son las que limitan la capacidad personal de los usuarios potenciales o sus incentivos para acceder a la conexión a internet donde está disponible o donde se ofrece, tal como los niveles de educación y alfabetismo.[139] Las barreras a la conectividad "rígidas" y "flexibles" se combinan para perpetuar la brecha digital dentro de los países, y por ende, a nivel global, aunque se presta mucha más atención generalmente a las barreras rígidas.

---

[134] Estudio de Stanford, *supra* nota 24, en 3.

[135] *Ibíd*.

[136] *Véase*, "India", *supra* nota 124 y texto acompañante (tabla 2. Acceso a internet con banda ancha fija o móvil); Estudio de Stanford, *supra* nota 24, en 3.

[137] *Véase*, Informe Mozilla, *supra* nota 24, en 5.

[138] *Véase*, Estudio de Stanford, *supra* nota 24, en 5; "Alliance for an Affordable Internet", The 2015-2016 Affordability Report, disponible en: http://bit.ly/2epYu5r; "Lifting Barriers to Internet Development in Africa: Suggestions for Improving Connectivity 16, Internet Society, 2013, disponible en: http://bit.ly/1MRw17S (de aquí en adelante, Internet Society, Lifting Barriers).

[139] Estudio de Stanford, *supra* nota 24, en 5; Informe Mozilla, *supra* nota 24, en 6.

Existen varios factores que actúan como barreras rígidas contra una mayor conectividad a internet en los países en vías de desarrollo, en gran parte por la falta de infraestructura técnica, los costos elevados y la accesibilidad. Se necesitan niveles altos de inversiones públicas y privadas para crear un sistema de internet alámbrico que funcione, y las condiciones políticas y económicas necesarias, por lo general, no están presentes. Por ejemplo, con un par de cableados submarinos tendidos hacia los países africanos, en general, crear conectividad fija resulta costoso, quizás hasta imposible para los estados más pobres.[140] Esto ayuda a explicar por qué el acceso a banda ancha alámbrico en Zambia es menor al 1% de la población. Incluso en Sudáfrica, el país más rico de la África subsahariana, apenas un poco más del 3% de la población está conectada de esta manera.[141] Esto se debe al hecho de que gran parte de la población rural vive a distancias muy alejadas del nodo más cercano en una red de fibra.[142] Si bien un incremento reciente en el cableado submarino ha contribuido con la difusión de internet en algunos partes del continente africano, los países del interior se ven forzados a depender de un poste que se encuentra en una estación de cableado terrestre en un país vecino.[143] Para resumir, "hay evidencia importante de que las conexiones terrestres transnacionales son insuficientes en África, y aquellas conexiones disponibles no son explotadas en su totalidad".[144]

Otras regiones del mundo enfrentan desafíos similares, y mantienen el acceso a internet fijo a niveles bajos o incluso insignificantes. En India, menos del 2% de la población cuenta con acceso alámbrico; en Malasia y Colombia, esa cifra apenas supera el 10%; en contraposición, las suscripciones alámbricas en los países desarrollados que formaron parte de la encuesta descripta más arriba llegan a un tercio, en promedio.[145] Parte del problema en los países en vías de desarrollo recae en el hecho de extender la conectividad a las zonas rurales, que suelen ser extensas. En China el 63% de la población que no está conectada se encuentra en zonas rurales.[146] En India, aproximadamente el 45% de la población rural no tiene electricidad.[147] Incluso en aquellos lugares donde está disponible, el acceso a banda ancha

[140] Internet Society, Lifting Barriers, *supra* nota 138, en 7.

[141] *Véase*, *supra* nota 121 y texto acompañante (tabla 2. Acceso a internet con banda ancha fija o móvil).

[142] Internet Society, Lifting Barriers, supra nota 138 , en 8.

[143] *Ibíd*. en 5-7.

[144] *Ibíd*. en 7.

[145] *Véase*, *supra* nota 121 y texto acompañante (Tabla 2: Acceso a internet con banda ancha fija o móvil).

[146] *Ibíd*.

[147] Internet Society, Lifting Barriers, *supra* nota 138, en 23.

alámbrica puede llegar a ser muy costoso. Una suscripción a banda ancha cuesta alrededor de 60 dólares mensuales en Australia y Mozambique.[148] No obstante, el ingreso anual bruto promedio en Australia es de 50.000 dólares estadounidenses; en Mozambique, menos de 500. Un plan de banda ancha con una velocidad de 25 a 50 MBPS en la ciudad de México costaba en promedio 123,73 dólares estadounidenses en 2014, mientras que en Ámsterdam costaba solamente 43,53 dólares estadounidenses.[149] México tiene un PBI per cápita de 10.325,6 y Holanda de 52.172,2. Y estas cifras no incluyen los gastos relacionados que se asocian con el acceso alámbrico en la compra de un dispositivo que permita tener internet, tal como una computadora personal o una tableta. Debido a estas razones, la penetración de banda ancha alámbrica es baja a insignificante en muchos países en vías de desarrollo, en donde, generalmente, se reserva para las élites urbanas y económicas.[150]

La falta generalizada de infraestructura física sumada al gasto de obtener acceso alámbrico donde existe, lleva a que cada vez más las personas en países en vías de desarrollo usen teléfonos móviles para poder acceder a internet.[151] Pero también existen obstáculos significativos para el acceso móvil. "En cuanto a la infraestructura, a pesar de los claros beneficios en la cobertura, en años recientes […] muchas personas siguen sin tener acceso: el 10% de la población mundial carece de acceso a servicios básicos de voz y texto, y apenas el 30% carece de acceso a internet de banda ancha móvil de 3 G/4 G. Cabe mencionar que la gran mayoría de esta población sin cobertura es de bajos recursos y vive en regiones rurales de Asia y África subsahariana".[152] El costo sigue siendo otra barrera importante.[153] Incluso

[148] Graham, Mark, "Broadband Affordability", *Geonet*, 7 de septiembre de 2014, disponible en: http://bit.ly/2gCXXiS.

[149] Russo, Nick, y Morgus, Robert *et al.*, "The Cost of Connectivity 2014", Open Technology Institute 17, 2014, disponible en: http://bit.ly/1or1N17.

[150] Informe Mozilla, *supra* nota 24, en 5-6.

[151] Informe Mozilla, *supra* nota 24, en 5-6; "Global internet Report 2015: Mobile Evolution and the Development of the Internet 24", Internet Society, disponible en: http://bit.ly/1JSpGVz; McKinsey y Company, "Offline and Falling Behind: Barriers to internet Adoption 16", 2014, disponible en: http://bit.ly/Ztobeu. Mientras que tan solo un cuarto de los usuarios en los países desarrollados tiene acceso a internet principalmente a través de un teléfono móvil, en países como Egipto y India ese número es aún mayor, 70% y 59% respectivamente.

[152] Informe Mozilla, *supra* nota 24, en 6.

[153] Véase, *ibíd*. La falta de infraestructura, e incluso los apagones, pueden afectar la cobertura celular. West, *supra* nota 50, en 3-4. Además, no todas las conexiones tienen la misma calidad. Si bien el 94% de la población rural en Holanda está cubierta por, al menos, una red móvil 3G, solo el 1% está cubierto en Zambia. International Telecommunications Union, "Measuring the Information Society Report 8", 2014, disponible en: http://bit.ly/1xrVMi8.

donde hay más disponibilidad de acceso móvil que de banda ancha fija, resulta costoso comparado con los ingresos locales.[154]

En promedio, los costos de banda ancha móvil en los países en vías de desarrollo son el doble que en los países desarrollados.[155] En los países en vías de desarrollo, las personas pueden gastar "entre 8-12% de su ingreso mensual promedio en conectividad móvil, y con frecuencia solo para servicios de voz y texto".[156] En Zimbabue o en la República Democrática del Congo, por ejemplo, el plan de datos promedio equivale al 100% del índice PBN mensual de ese país.[157] De manera similar, en lugares como India, una persona promedio necesitaría trabajar 17 horas para poder costear un plan de datos móviles de 500 MB, comparado con las tres horas de salario mínimo que se necesitaría en los Estados Unidos para obtener un plan de datos ilimitado por un mes.[158] En Zambia, un plan de datos móviles de 500 MB cuesta 200 veces más de lo que costaría en promedio un galón de leche.[159] Comparemos eso con Holanda, donde un paquete de 500 MB y llamadas y textos ilimitados cuestan 25 libras esterlinas por mes y el salario mínimo para una jornada semanal de 36 a 40 horas es de 351,85 libras esterlinas.[160]

Para resumir, tanto en el contexto de acceso a internet con banda ancha alámbrica como con teléfono móvil, los costos elevados son el mayor obstáculo para la mayoría de los consumidores en el mundo en vías de desarrollo. En el caso del acceso móvil es, sin dudas, el principal. La mayoría de las personas no tienen los recursos necesarios para tener un plan de datos costoso y pagar las tarifas que corresponden al acceso a internet desde un teléfono básico o uno que no sea inteligente, y mucho menos tienen un teléfono inteligente costoso.[161] Afortunadamente, los teléfonos inteligentes cada vez son más accesibles, y casi no quedan dudas de que representan el futuro de la conectividad móvil en el

[154] Carew, Diana, Progressive Policy Institute, "Zero-Rating: Kick-Starting Internet Ecosystems in Developing Countries 1", 2015, disponible en: http://bit.ly/2gMpxe4.

[155] International Telecommunication Union, "ICT Facts and Figures 4", 2015, disponible en: http://bit.ly/1FOoa6p.

[156] Carew Diana, Progressive Policy Institute, "Zero-Rating: Kick-Starting internet Ecosystems in Developing Countries 3", 2015, disponible en: http://bit.ly/2gMpxe4.

[157] Mahapatra, Lisa, "Data Plans: Developed Countries Have the Most Affordable Mobile Broadband Plans", *Int'l Business Times*, 11 de octubre de 2013, disponible en: http://bit.ly/2g5qDBM.

[158] Eagle, Nathan, "How to Make the internet Free in Developing Countries", Tech Crunch, 1 de junio de 2015, disponible en: http://tcrn.ch/2gMjHcP.

[159] *Véase*, *infra* notas 170-200.

[160] Gobierno de Holana, "Minimum Wage", disponible en: http://bit.ly/2fMeBMN. Lycamobile, "Bundle Offers", disponible en: http://bit.ly/2bpKqeX.

[161] West, *supra* nota 50, en 2.

mundo en vías de desarrollo.[162] Lo que resulta más sorprendente, sin embargo, es que aun cuando las personas tienen acceso a una conexión a internet, eligen no usarla, o son incapaces de hacerlo. Estas son las barreras flexibles al acceso.

La falta de alfabetización en diversas formas constituye un impedimento para muchos usuarios. Los usuarios que carecen de alfabetización digital, por ejemplo, pueden experimentar "desconocimiento o incomodidad al usar tecnologías digitales con el fin de acceder a la información y hacer uso de ella".[163] Pero si el usuario potencial no puede leer ni escribir, la tarea de conectarse a internet será aún más difícil.[164] Las tasas de alfabetización en este aspecto tienden a ser menores –aunque no siempre en gran medida– en los países en vías de desarrollo encuestados comparados con los países desarrollados.[165] Otra barrera es la relevancia: las personas son menos propensas a conectarse a internet si no ven o entienden su utilidad. Esto sucede, por ejemplo, donde no hay suficiente contenido que les resulte atractivo o que se relacione con su vida diaria.[166] Asimismo, las compañías en los países en vías de desarrollo con niveles bajos de conectividad móvil tienen muy poco incentivo para invertir en los servicios en línea precisamente porque hay pocos clientes que cuentan con acceso a internet.[167] Estos factores se conjugan para formar un *status quo* de "equilibrio de conectividad baja" que puede ser difícil de sobrellevar.[168] La proliferación en los países en vías de desarrollo de usuarios de teléfonos móviles, en general, y de usuarios de teléfonos inteligentes en particular, no será tan efectiva como podría serlo a fin de cerrar la brecha digital, a menos que se combine con ofertas de contenido local relevantes y programas de alfabetización digital dirigidos a nuevos suscriptores.[169]

I.B.III. Tres abordajes sobre el *zero-rating*

El análisis precedente utiliza datos cuantitativos para ilustrar los diferen-

[162] *Véase*, Informe Mozilla, *supra* nota 24, en 6-11.

[163] McKinsey, supra nota 151, en 4.

[164] *Ibíd*.

[165] *Véase*, tabla 3, *supra* nota 125. Si bien algunas tecnologías, como texto a voz o reconocimiento de voz pueden facilitar la navegación incluso para los usuarios analfabetos, a la mayoría de los usuarios que no tienen un nivel básico del idioma les puede resultar difícil relacionarse con internet de manera significativa. McKinsey, *supra* nota 151, en 42.

[166] West, *supra* nota 50, en 5; Internet.org, "State of Connectivity: 2014: A Report on Global internet Access 30", 2014, disponible en: http://bit.ly/1EE9B0E. Por supuesto, si el acceso no está disponible en los idiomas locales eso desalentará aún más el acceso.

[167] Carew, *supra* nota 154, en 3.

[168] *Ibíd*.

[169] Informe Mozilla, *supra* nota 24, en 34-35.

tes contextos donde existen políticas de neutralidad de la red y prácticas de *zero-rating* en el mundo. En esta subsección, nos enfocamos específicamente en tres de los países examinados previamente, cada uno refleja un abordaje distinto sobre el *zero-rating*. Dichos países son Zambia, Chile y Estados Unidos. El estudio sobre cada país integra los datos pertinentes desde el punto de vista económico, político y tecnológico a partir de la subsección precedente con información adicional sobre cómo se abordó la neutralidad de la red, en términos generales, y el *zero-rating*, en términos particulares.

I.B.III.A. Zambia

Un ejemplo de nación en vías de desarrollo que acepta el *zero-rating* es Zambia, en el sur de África, que posee un sistema democrático débil. Es una república presidencial, pero a lo largo de gran parte de su historia de independencia, Zambia ha sido controlada por un único partido político, el Partido Unido de la Independencia Nacional (UNIP, según sus siglas en inglés). Zambia pasó por un período de descentralización a principios de la década de los 90 y ha sufrido reformas económicas desde comienzos del 2010[170]. Sin embargo, el clima político en Zambia no es totalmente libre según el Informe Mundial sobre Libertad 2016 realizado por Freedom House.[171]

Con respecto al desarrollo humano, Zambia ha quedado rezagada, a pesar del aumento significativo en su índice de desarrollo humano (IDH), que va desde el año 2012 al 2013. Como se puede observar en la Parte I.B (tabla 3), en el año 2013 Zambia se encontraba en la parte más baja del rango de desarrollo medio, en el puesto 141 de una lista de 187 naciones clasificadas según su IDH.[172] En 2012, no obstante, ocupó el puesto 163 con un IDH menor que el promedio para los países con "desarrollo bajo", así como también para las naciones subsaharianas.[173] De cualquier modo, el PBI per cápita de ese país es el más bajo de todas las naciones evaluadas.[174] Por dicha razón, entre otras, las Naciones Unidas sigue incluyendo a Zambia dentro de las

[170] "Zambia Among World's Fastest Growing Economies. World Bank", Lusaka Voice, 16 de abril de 2013, disponible en: http://bit.ly/2fJlUrV.

[171] "Freedom of the Press: Zambia 2016 Scores", Freedom House. Disponible en: http://bit.ly/2eNZrtf.

[172] *Véase*, *supra* nota 128 y texto acompañante.

[173] PNUD, Zambia Country Profile, "The Rise of the South: Human Progress in a Diverse World 2", 2013, disponible en: http://bit.ly/2fbJN9L.

[174] *Véase*, *supra* nota 126 y texto acompañante.

48 naciones "menos desarrolladas" del mundo desde 2014.[175]

Zambia permite el *zero-rating*: fue el primer país en donde Facebook implementó Internet.org en julio del 2014.[176] El país aparentemente no cuenta aún con un marco legal o político concreto en términos de neutralidad de la red.[177] En general, la neutralidad de la red (aún) no está regulada en muchos países africanos.[178] La Internet Service Providers' Association (Asociación de Proveedores de Servicios de Internet) expresó que la neutralidad de la red "no es un problema" en muchos países como Sudáfrica.[179] Algunos sostienen que las leyes sobre neutralidad de la red abordan la calidad del acceso y que solamente llegan a ser relevantes cuando existe una gran cantidad de acceso.[180] Argumentan esto como la razón por la cual las leyes sobre neutralidad de la red no se han propagado por toda África.[181] Mientras los opositores a las regulaciones más estrictas sobre neutralidad de la red en países africanos aceptan que el *zero-rating* complicará a los nuevos emprendimientos y facilitará a las grandes compañías en su tarea por dominar el mercado, creen que "el mal acceso supera la falta de acceso cada día de la semana".[182]

Internet.org opera en Zambia a través de Airtel, un proveedor privado de telecomunicaciones.[183] Además de ofrecer servicios como Facebook, Messenger, AccuWeather, Google Search y Wikipedia, Internet.org les brinda a los habitantes de Zambia acceso al sitio para la salud y la nutrición de UNICEF, incluso información sobre VIH/SIDA (Zambia uReport). Otras aplicaciones incluyen un sitio sobre deportes, un sitio sobre servicios de noticias independientes y una aplicación sobre los derechos de las mujeres.[184] Wikimedia Zero no opera en

[175] *Véase*, *supra* notas 125-128 y texto acompañante (debate el criterio y la lista actual de los países menos desarrollados de las Naciones Unidas).

[176] Rosen, *supra* nota 79.

[177] *Véase*, "Freedom on the Net 2015", Freedom House, disponible en: http://bit.ly/2gYLZU7 (detalla el marco legal que se aplica a las regulaciones sobre internet en Zambia, sin mencionar las normas sobre neutralidad de la red).

[178] Van Zyl Gareth, "Is Net Neutrality a 'Non-Issue' in Africa?", IT Web Africa, 18 de agosto de 2014, disponible en: http://bit.ly/1kQZG45.

[179] "'Net Neutrality' a Non-Issue in South Africa for the Present, Says ISPA", ISPA, 11 de agosto de 2014, disponible en: http://bit.ly/2gYUaA1.

[180] Song, Steve, "Net Neutrality in Africa", Many Possibilities, 7 de mayo de 2014, disponible en: http://bit.ly/2gD0M3l.

[181] *Ibíd*.

[182] *Ibíd*.

[183] *Ibíd*. "Company Overview of Airtel Networks Zambia Plc", *Bloomberg Business*, disponible en: http://bloom.bg/2f7Seji.

[184] Honan, Mat, "Facebook-Backed Non Profit Brings Free internet to Zambia", *Wired*, 31 de julio de 2014, disponible en: http://bit.ly/2gYVEKp. *Véase*, además, Rosen, *supra* nota 79.

Zambia en la actualidad.[185] La llegada de Internet.org es significativa ya que, históricamente, Zambia ha tenido tasas bajas de penetración de internet. Entre 2010 y 2014, el porcentaje de usuarios de internet en Zambia superó el 50%, pero el total tan solo llegó al 15,4% de la población.[186] De alguna manera, logró alcanzar el 17%.[187] En su territorio, Zambia tiene solamente cuatro servidores seguros para un millón de personas.[188] A partir de 2010, solo el 1,3% de la población tiene acceso a internet desde su hogar y menos de 4% tiene una computadora en su hogar.[189] No obstante, más del 50% de los hogares tiene teléfonos móviles celulares.[190] Por esas razones, Zambia ocupa el puesto 144 de los 166 países incluidos en el índice sobre desarrollo de la tecnología de la Información y de la Comunicación que proporciona el International Telecommunication Union.[191]

Si bien el sector de las telecomunicaciones en Zambia es limitado, se encuentra en un período de crecimiento. Desde la década de los 90, ha contado con un solo proveedor de servicios de internet privado pero están surgiendo nuevas compañías.[192] Asimismo, el ente regulador de telecomunicaciones, Zambia Information and Communications Technology Authority, es nominalmente independiente.[193] Su misión comprende la regulación, el monitoreo, la fijación de normas y la promoción de la competencia en el sector de las telecomunicaciones.[194] Uno de los objetivos estratégicos es fomentar el acceso universal en la población.[195] Desafortunadamente, Zambia es uno de los países más corruptos de todos los países analizados, a la par con India y apenas mejor que Colombia.[196] En términos generales, Transparency International (TI) lo ubica en el puesto 85 de 175 países en el mundo.[197]

---

[185] *Véase*, "Mobile Partnerships", *supra* nota 32

[186] "Internet Users", *supra* nota 124.

[187] "Freedom on the Net 2015", *supra* nota 177; "Emerging Nations Embrace internet, Mobile Technology", Pew Research Center, 13 de febrero de 2014, disponible en: http://pewrsr.ch/2gc4S1R.

[188] "Secure Internet Servers (per 1 million people)", Banco Mundial, disponible en: http://bit.ly/2gnMfMj.

[189] ITU, *supra* nota 122.

[190] *Ibíd*.

[191] "MIS 2014 Report Charts", tabla 2.1, ITU, disponible en: http://bit.ly/1FltDj5.

[192] "Zambia Telecommunications", Pricewaterhouse Cooper, disponible en: http://pwc.to/2fPuYab.

[193] *Ibíd*.

[194] "About Us", Zambia Information & Communications Technology Authority, disponible en: http://bit.ly/1j0n1PX.

[195] *Ibíd*.

[196] *Véase*, *supra* tabla 4.

[197] "Corruption Perceptions Index 2014", Transparency Int'l, disponible en: http://bit.ly/1AgRivL. *Véase*, *supra* tabla 4, disponible en: http://bit.ly/2g422z5.

Existen dos obstáculos principales para lograr una mayor conectividad a internet en Zambia: el primero es de carácter económico y el segundo se relaciona con la infraestructura. Como Zambia es un país menos desarrollado (PMD), los ingresos nacionales son muy bajos y a las personas les resulta difícil gastar dinero en acceso a internet en lugar de hacerlo en otras necesidades apremiantes. Por ejemplo, mientras que un galón de leche en Zambia cuesta el equivalente a 4,6 dólares estadounidenses, un paquete de datos de internet móvil de 500 MB para 30 días cuesta aproximadamente 20 dólares estadounidenses.[198] Además, Zambia tiene una elevada carga impositiva sobre el acceso a internet –la relación pagos impositivos/ganancias de operadores de redes móviles es de 53%–.[199] Las limitaciones en la infraestructura también obstaculizan un mayor acceso. Como Zambia es una nación interna, no tienen acceso a cableado submarino, algo que podría elevar la competencia y reducir el precio.[200] Con el propósito de tener acceso a esos cables, Zambia tendría que depender de países vecinos costeros, lo cual no es viable en muchas ocasiones.[201]

I.B.III.B. Chile

Chile fue la primera nación del mundo en adoptar una ley sobre la neutralidad de la red en 2010.[202] Es un país de América del Sur con un sistema democrático consolidado que se basa en elecciones populares y en un sistema político multipartidario. Tiene un sistema presidencial con leyes sancionadas por el Congreso e implementadas por el presidente. Freedom House califica a Chile como "libre" con la máxima calificación tanto en libertades civiles como en derechos políticos,[203] mientras que la libertad de prensa clasifica solo como "parcialmente libre", en parte por la falta de competencia en el mercado de medios.[204] Los niveles de corrupción son relativamente bajos, especialmente según las normas regionales. La Transparency International posiciona a Chile

[198] *Véase*, "Cost of Living in Zambia", Numbeo, disponible en: http://bit.ly/1lLdRtt. *Véase*, además, "MTN Zambia Mobile internet Data Sheet", GitHub Gist.

[199] McKinsey & Company, *supra* nota 151, en 41.

[200] *Ibíd*. en 47.

[201] *Ibíd*.

[202] Walker, Lauren, "How Is Net Neutrality Working for the Countries That Have It?", *Newsweek*, 10 de septiembre de 2014, disponible en: http://bit.ly/1lWlkov

[203] "Freedom in the World: Chile 2014 Scores", Freedom House, disponible en: http://bit.ly/2foB5Tm.

[204] "Freedom of the Press: Chile 2014 Scores", Freedom House, disponible en: http://bit.ly/2gnPTpz.

en el puesto 21 de 175 países en términos de corrupción y, junto con Uruguay, ocupa los niveles más bajos de América del Sur.[205] A pesar del PBI promedio per cápita, Chile se posiciona en un nivel alto en cuanto al desarrollo humano. Según el PNUD, Chile ocupa el lugar 41 de 187 naciones y tiene el nivel más alto en términos de desarrollo humano en América del Sur.[206]

Respecto del desarrollo económico, las Naciones Unidas clasifica a Chile como una economía en vías de desarrollo con ingresos elevados (mejorando el nivel de ingresos medio alto que tenía en 2014).[207] Chile llegó a ser miembro de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en el año 2010 –el primer país de América del Sur en ser miembro–.[208] Sin embargo, Chile también tiene un nivel de desigualdad elevado, según reveló el Banco Mundial, que le dio a Chile un puntaje de 50,8 en términos del índice GINI (donde 0 es la igualdad perfecta y 100 es la desigualdad perfecta).[209]

Como se ha señalado, Chile fue la primera nación del mundo en adoptar una ley sobre la neutralidad de la red en 2010,[210] que prohíbe la mayoría de los tipos de *zero-rating*. A nivel normativo, las disposiciones establecidas por ley crean una prohibición "general" para prácticas que violan la neutralidad de la red.[211] Las leyes sobre neutralidad de la red en Chile establecen que los proveedores de servicios de internet (ISP) no podrán, "de manera arbitraria bloquear, interferir, discriminar, ocultar o restringir contenido, aplicaciones o servicios legales que los usuarios realicen en sus redes".[212] En principio, la prohibición legal sobre discriminación comprendía a las aplicaciones de redes

[205] Transparency Int'l, *supra* nota 196; véase, *supra* tabla 2.

[206] Progama de las Naciones Unidas para el Desarrollo, "Chile: Human Development Indicators", disponible en: http://hdr.undp.org/en/countries/profiles/CHL Véase, "United Nations Development Programme", International Human Development Indicators, disponible en: http://bit.ly/1rAOGrY (mapa que muestra Argentina como la nación que le sigue en la clasificación, ocupando el puesto 49 en América del Sur).

[207] "Country Classification", Naciones Unidas, disponible en: http://bit.ly/1VctxnS.

[208] "Members and Partners", OCDE, disponible en: http://bit.ly/2gYV0N3. Chile Signs up as First OECD Member in South America", OCDE, 1 de noviembre de 2010, disponible en: http://bit.ly/2g42bCR.

[209] "GINI Index (World Bank estimate)", Banco Mundial, disponible en: http://bit.ly/TLu3fJ. "Consagra el principio de neutralidad en la red para los consumidores y usuarios de internet, general de telecomunicaciones", Ley No. 18.168, 26 de agosto de 2010, disponible en: http://bit.ly/1msnmfa. Walker, *supra* nota 201.

[210] *Ibíd*.; Walker, *supra* nota 201, Subsecretaría de Telecomunicaciones, Circular 40 (Chile), disponible en: http://bit.ly/2g5Sodt; Walker, *supra* nota 201.

[211] Subsecretaría de Telecomunicaciones, Circular 40 (Chile), disponible en: http://bit.ly/2g5Sodt. Walker, *supra* nota 201.

[212] "Chile: First Country to Legislate Net Neutrality", Global Voices, 4 de septiembre de 2010, disponible en: http://bit.ly/2fPun8o.

sociales comúnmente ofrecidas con *zero-rating*, como Twitter, WhatsApp y Facebook.[213] En 2014, la Subsecretaría de Telecomunicaciones de Chile (Subtel), el ente regulador de telecomunicaciones, anunció que dichos servicios ya no estaban permitidos, y que toda compañía que los utilizara sería pasible de multas.[214] De igual modo, Internet.org fue cerrada.[215] Si bien los activistas por la neutralidad de la red estaban complacidos por el abordaje tomado en Chile, otros lo calificaron de cortoplacista.[216] Haciendo referencia a la tasa elevada de uso de teléfonos móviles en Chile y la tasa baja de uso de internet móvil y alámbrica, los opositores sostienen que el plan chileno carece de "matices" y dificultaría el crecimiento del acceso a internet en el país.[217]

Sin embargo, en la práctica, la ley sobre neutralidad de la ley en Chile, hoy en día, solamente prohíbe la aplicación del *zero-rating* por parte de los operadores móviles de aplicaciones y servicios de redes sociales que se ofrecen como promociones o planes comerciales.[218] Algunas formas de *zero-rating* siguen existiendo o son permitidas por Subtel, incluso las plataformas de redes sociales de *zero-rating.*[219] Particularmente, Subtel emitió su opinión y expresó que Wikipedia Zero no violaba los términos de la ley ni la interpretación de Subtel sobre la protección de la neutralidad de la red.[220]

A diferencia de la mayoría de los países en vías de desarrollo, Chile tiene una penetración de internet significativa. A partir de 2013, más del 66% de la población tiene acceso a internet, con 94 servidores seguros para 1 millón de personas.[221] Aproximadamente el 70% de la población accede a internet en forma diaria,[222] lo que confirma que Chile enfrenta muy pocas barreras específicas en cuanto a la conectividad a internet. A partir de 2011,

[213] Moody, Glyn, "Chile Bans Free Delivery of Social Media Services to Uphold Net Neutrality", TechDirt, 16 de junio de 2014, disponible en: http://bit.ly/1DkxFGK. "Ley de Neutralidad y Redes Sociales Gratis", Subsecretaria de Telecomunicaciones, 27 de mayo de 2014, disponible en: http://bit.ly/1CP17UL.

[214] Meyer, David, "In Chile, Mobile Carriers Can No Longer Offer Free Twitter, Facebook or WhatsApp", Gigaom, 28 de mayo de 2014, disponible en: http://bit.ly/2fDszCY.

[215] Informe Public Knowledge de Rossini y Moore, *supra* nota 24, en 17-18.

[216] Mirani, Leo, "When Net Neutrality Backfires: Chile Just Killed Free Access to Wikipedia and Facebook", Quartz, 30 de mayo de 2014, disponible en: http://bit.ly/2gD2rWD.

[217] *Ibíd*.

[218] Informe Public Knowledge de Rossini y Moore, *supra* nota 24, en 19-20.

[219] *Ibíd*. *Véase*, por ejemplo, ClaroChile, disponible en: http://bit.ly/1PDuP4J.

[220] *Ibíd*.

[221] Usuarios de internet (cada 100 personas)", *supra* nota 124; "Secure internet Servers (per 1 million people)", Banco Mundial, disponible en: http://bit.ly/2gnMfMj.

[222] "Emerging Nations", *supra* nota187.

más del 40% de los hogares tenía acceso a internet en sus viviendas.[223] La infraestructura del país sufrió un golpe duro con el terremoto de febrero de 2010, pero se conjugaron esfuerzos públicos y privados para invertir en la reconstrucción.[224] Si bien más del 90% de los chilenos tienen un teléfono celular, solo el 39% tiene un teléfono inteligente.[225] Sin embargo, el 55% de los ciudadanos chilenos entre 18 y 29 años tiene un teléfono inteligente, esto sugiere que la división es generacional.[226] Finalmente, el sector de las telecomunicaciones en Chile está privatizado.[227] Como hemos observado, Subtel regula la industria, incluso emite licencias y promulga normas.[228]

I.B.III.C. Los Estados Unidos

Los Estados Unidos clasifica como nación democrática libre y como la mayor economía mundial. Algunas revelaciones recientes sobre vigilancia masiva del gobierno han generado preocupación en términos de privacidad y libertad en el uso de internet.[229] La corrupción es relativamente baja (el país ocupa el puesto 17 entre 175 naciones según TI).[230] Conforme al Informe de Desarrollo Humano, los Estados Unidos es una nación desarrollada. Goza de un gran desarrollo humano, ocupa el puesto 5 entre 166 países.[231] Asimismo, los Estados Unidos tiene el puntaje más elevado en cuanto a desarrollo humano en el continente americano.[232]

Los Estados Unidos no prohíbe el *zero-rating,* pero la inclinación por la neutralidad de la red requiere que dichas prácticas sean revisadas para

[223] *International Telecommunication Union* (ITU), "Core Indicators on Access to and Use of ICT by Households and Individuals (Excel)", disponible en: http://bit.ly/1cblxxY (de aquí en adelante Indicadores claves).

[224] *Ibíd*.

[225] "Emerging Nations", *supra* nota 187.

[226] *Ibíd*.

[227] *Véase*, Informe Public Knowledge de Rossini y Moore, *supra* nota 24, en 15-20 (describe la regulación de Chile de las compañías de telecomunicaciones privadas en ese país).

[228] *Ibíd*.

[229] "Freedom on the Net: United States 2014 Scores", Freedom House, disponible en: http://bit.ly/2eOi2FN.

[230] Transparency Int'l, *supra* nota 196; *véase*, *supra* tabla 2.

[231] Programa de las Naciones Unidas para el Desarrollo, "United States: Human Development Indicators, Human Development Reports", disponible en: http://bit.ly/1N0VQnb.

[232] *Véase*, *supra* tabla 3.

salvaguardar posibles consecuencias injustas o perjudiciales.[233] En sus normas de internet abierta 2015, la Comisión Federal de Comunicaciones adoptó un marco extremadamente protector de la neutralidad de la red para regular internet en varios aspectos.[234] En primer lugar, la Comisión Federal de Comunicaciones definió que las nuevas normas alcanzan "tanto al servicio de acceso a internet fijo como móvil".[235] En segundo lugar, la Comisión Federal de Comunicaciones sancionó tres normas claras que apuntan a proteger específicamente la neutralidad de la red prohibiendo: los bloqueos;[236] la limitación de ancho de banda;[237] y la priorización según los precios.[238] Finalmente, la Comisión Federal de Comunicaciones estableció un modo de lograr otros tipos de conducta que no entran en las tres normas claras mediante el establecimiento de su "estándar de interferencia/desventaja razonable".[239] Conforme a este estándar, los proveedores de servicios de

[233] *Véase*, Carrillo, Arturo J., y Nunziato, Dawn C., "The Price of Paid Prioritization: The International and Domestic Consequences of the Failure to Protect Net Neutrality in the United States", *Georgetown Journal Int'l Affairs*, verano de 2015, 98, 98, disponible en: http://bit.ly/2gc4tMM.

[234] "Net Neutrality: President Obama's Plan for a Free and Open Internet", White House, disponible en: http://bit.ly/2gq7wUS.

[235] Normas de internet abierta 2015, *supra* nota 2, en ¶ 25.

[236] *Ibíd*. ¶ 112. "La persona que se dedica a brindar servicios de acceso a internet con banda ancha, siempre que esa persona se dedique realmente a ello, no deberá restringir contenido, aplicaciones, servicios legales o dispositivos no perjudiciales con sujeción a una administración de la red razonable".

[237] *Ibíd*. ¶ 119. "La persona que se dedica a brindar servicios de acceso a internet con banda ancha, siempre que esa persona se dedique realmente a ello, no deberá impedir o degradar el tráfico de internet no lícito sobre la base del contenido, la aplicación o el servicio de internet, o usar dispositivos no perjudiciales, con sujeción a una administración de la red razonable".

[238] *Ibíd*. ¶ 125. "La persona que se dedica a brindar servicios de acceso a la internet con banda ancha, siempre que esa persona se dedique realmente a ello, no deberá ofrecer priorización según precios. El término 'priorización según precios' hace referencia a la administración de la red del proveedor de red de banda ancha, directa o indirectamente, para favorecer cierto tráfico sobre otro, incluso a través del uso de técnicas como modelado de tráfico, priorización, reserva de recursos u otras formas de administración de tráfico preferencial, ya sea (a) a cambio de una contraprestación (pecuniaria o de otra índole por parte de terceros), o (b) para beneficio de una entidad afiliada".

[239] *Ibíd*. ¶ 136. "La persona que se dedica a brindar servicios de acceso a internet con banda ancha, siempre que esa persona se dedique realmente a ello, no deberá de manera no razonable interferir con o desfavorecer de manera no razonable (i) la habilidad de los usuarios finales de seleccionar, acceder y usar el acceso a internet con banda ancha o a contenido, aplicaciones, servicios de internet legales, o dispositivos de su elección, o (ii) la habilidad de los proveedores para hacer que el contenido, las aplicaciones, los servicios o dispositivos legales estén disponibles para los usuarios finales. La administración razonable de la red no deberá ser considerada como una violación a esta norma".

internet no pueden interferir de manera no razonable o con desventaja en la habilidad de los usuarios finales de usar y acceder al servicio de banda ancha o al contenido de internet o en la habilidad de los proveedores de hacer que ese contenido esté disponible.[240] En otras palabras, la Comisión Federal de Comunicaciones decidió que no aplicaría la norma clara de prohibir rotundamente los datos patrocinados o los planes con *zero-rating* sino que, en su lugar, evaluaría este tema caso por caso en relación con el "estándar de interferencia/desventaja razonable".[241]

La penetración de internet es elevada en todos los Estados Unidos, desde las zonas metropolitanas hasta las rurales. En 2014, los Estados Unidos superaron a todos los demás países examinados por la OCDE en cuanto a cobertura de internet, con un total de 100.192.000 suscripciones de banda ancha inalámbrica y fija.[242] Con respecto a las suscripciones para 100 personas ocupó el puesto 16, Corea y Nueva Zelanda fueron los únicos países no europeos en tener un número elevado de suscripciones de banda ancha inalámbrica y fija.[243] El 84% del país tiene acceso, el 68% de los adultos tiene acceso a través de conexiones móviles y el 70% de los hogares tiene banda ancha de alta velocidad.[244] En la actualidad, el acceso y los servicios *zero-rating* dependen de las distintas opciones que ofrecen los operadores privados de redes móviles. T-Mobile, por ejemplo, aplica *zero-rating* a ciertas aplicaciones de música para algunos de sus planes de datos, pero no para otras.[245]

I.C. Observaciones finales

En esta segunda parte, elaboro un análisis de los diferentes tipos de prácticas *zero-rating* del sector privado y las organizo en cuatro categorías básicas: sitio único, compuesta, datos patrocinados y falsa o no selectiva. He presentado datos empíricos relacionados con el acceso a internet, la neutralidad de la red y el *zero-rating* en todo el mundo, así como también el contexto socioeconómico y político donde existen dichas cuestiones. Esto incluyó una encuesta sobre diversas barreras a la conectividad, especial-

[240] Norma de la internet abierta 2015, *supra* nota 2, p. ¶ 136.

[241] *Ibíd*. ¶ 152.

[242] "Broadband Portal", OECD, 23 de julio de 2015, disponible en: http://bit.ly/1cP4RGV.

[243] *Ibíd*.

[244] "Freedom on the Net: United States 2014 Scores", *supra* nota 229.

[245] Molen, Brad, "On T-Mobile, You Can Now Stream Music without Hurting Your Data Plan", Engadget, 18 de junio de 2015, disponible en: http://engt.co/2gpZH1t. *Véase* además, *supra* notas 61-63 y texto acompañante.

mente los costos elevados asociados con el acceso a internet en los países en vías de desarrollo, que es una pieza esencial del enigma del *zero-rating*. Y, al observar todos esos datos a través de la mirada de tres estudios de casos representativos, espero haber explicado adecuadamente los enfoques principales considerados o adoptados por ciertos países en el mundo en el intento por regular la neutralidad de la red y el *zero-rating*. Ahora estamos listos para abordar el tema del marco del derecho internacional.

II. "Nueva" perspectiva: el marco del derecho internacional

Si bien resulta importante mantener una internet abierta y libre, el principio de la neutralidad de la red es mucho más que eso. En la actualidad, es una norma bien establecida del derecho internacional de los derechos humanos, un elemento esencial de los derechos de libertad de expresión y no discriminación en línea. Pero, ¿cómo ha logrado llegar a esa instancia? Ningún tratado de derechos humanos menciona el término "neutralidad de la red", acuñado por Tim Wu, profesor de Derecho en los Estados Unidos, en 2003.[246] Más para señalar: ¿Por qué es importante? ¿Qué es significativo respecto de la evolución de la neutralidad de la red desde un principio normativo y una prioridad de política propuesta por los Estados Unidos hasta una norma de derechos humanos vinculante para los Estados? ¿Por qué los defensores y los críticos de la neutralidad de la red deberían –o en realidad, deben– entender las implicancias de esa norma sobre los derechos humanos hoy en día? Abordaremos dichas cuestiones y otras similares.

En esta parte, describo la evolución de la neutralidad de la red como norma de derechos humanos antes de incluirla en un marco legal para analizar esos derechos. Se divide en tres secciones. En la primera sección, respondo a la siguiente pregunta: ¿Cómo llegó la neutralidad de la red a ser una norma del derecho internacional de los derechos humanos? Esta sección inicial observa cómo la neutralidad de la red se convirtió en parte integral de la libertad de expresión, definida como el derecho a impartir, buscar y recibir información, por un lado y por el otro, el derecho de acceso a internet o la "conectividad". La segunda sección describe el marco legal contemporáneo, incluso las normas de la no discriminación y sus efectos sobre el derecho a la libertad de expresión. Además, explica el régimen de excepciones que establece el derecho de los derechos humanos para determinar en qué casos

[246] Wu, Tim, "Network Neutrality, Broadband Discrimination", Telecommunication & High Technology Law, Vol. 2, No. 141, Año 14, 2003.

se permiten las restricciones a los derechos fundamentales por parte de los Estados. En la tercera y última sección, respondo a la pregunta de por qué es importante, por no decir necesario, que tratemos la neutralidad de la red como lo que realmente ha llegado a ser: una norma multifacética del derecho moderno de los derechos humanos.

II.A. Cómo la neutralidad de la red llegó a ser una norma del derecho internacional de los derechos humanos

La neutralidad de la red no comenzó como un derecho humano. Hace décadas, el concepto de una red neutral de datos o "abierta" se incorporó a la incipiente internet desde su diseño.[247] Esta "apertura" comprende no solo la ingeniería en términos de programas y estándares sino de valores liberales de la libertad de expresión y el egalitarismo derivado del entorno donde se creó internet.[248] La internet "abierta" surgió para garantizar el flujo libre y no regulado de información de extremo a extremo es decir, sin interferencias sustanciales durante la transmisión de datos desde un usuario "inteligente" a otro, a través de simples cañerías o de la red física.[249] "Una consecuencia de este diseño es el principio de la no discriminación entre aplicaciones".[250] Otra consecuencia fue el crecimiento exorbitante y el gran éxito de internet como red de comunicaciones.[251] No es de sorprender que los primeros activistas anunciaban a internet como una gran fuerza liberadora, y en particular porque el "ciberespacio" era considerado libre de todo tipo de límites territoriales, regulaciones gubernamentales y controles económicos que azotaban a otros sistemas de comunicaciones.[252] Desde entonces ha quedado claro que ya no es más así, si es que alguna vez lo fue.[253]

Si bien el concepto estaba casi presente, el término neutralidad de la red no entró en el debate de la política de internet hasta el año 2003. Nació en

[247] Goldsmith, Jack, y Wu, Tim, "Who Controls the internet?: Illusions of a Borderless World", *Oxford University Press, Inc*., 2006, pp. 23 -25.

[248] *Ibíd*., en 19; *Véase además*, Lemley, Mark A., y Lessig, Lawrence, "The End of End-to-End: Preserving the Architecture of the internet in the Broadband Era", *UCLA Law Review*, No. 48, 925, 930, 2001;

[249] *Ibíd*., en 930-31. Sobre la naturaleza no regulada de la internet temprana. *Véase*, *además*, Lawrence Lessig, Code: Version 2.0, 2006, pp. 1-82 (de aquí en adelante, Código Lessig).

[250] Lemley y Lessig, *supra* nota 248, en 931.

[251] *Ibíd*.

[252] Goldsmith y Wu, *supra* nota 247, en 17-21.

[253] Véase, Lessig, Code, *supra* nota 249; Goldsmith y Wu, *supra* nota247; *Véase*, Morozov, Evgeny, *The Net Delusion: The Dark Side of internet Freedom*, Public Affairs, Perseus Book Group, New York, 2012.

medio de un debate en los Estados Unidos sobre la mejor forma de garantizar el "acceso abierto" a internet a través de regulaciones a la luz de los avances de los servicios de banda ancha en el cambio de siglo.[254] La preocupación residía en que al permitir la integración de los proveedores de servicios de internet y de contenido por parte de compañías de cable, el principio de "extremo a extremo" que como se remarcó anteriormente, había probado ser indispensable para el crecimiento extraordinario de internet, se interrumpiría.[255] Mientras que los defensores del "acceso abierto" proponían soluciones estructurales que apuntaban a preservar la arquitectura natural de internet (es decir, prohibir las fusiones propuestas[256]), Tim Wu propuso en su lugar la adopción de una directiva política –la neutralidad de la red– que era la "expresión concreta de un sistema de creencias sobre la innovación".[257] Al hacerlo, le asignó un nombre a la naturaleza no discriminatoria del principio de "extremo a extremo" en el núcleo de la internet "abierta". En otras palabras, Wu buscaba cambiar los términos del debate de los Estados Unidos sobre la mejor forma de preservar las virtudes de una internet "abierta" lejos de toda discusión relacionada con la necesidad de soluciones estructurales hacia una política normativa y el principio a favor de la competencia de la neutralidad de la red.[258] Tuvo éxito.[259]

Es poco probable que los defensores académicos de los principios de la neutralidad de la red en los Estados Unidos durante la década del 2000 pudieran haber previsto el impacto internacional de su creación. Sin embargo, alrededor de 2015, el concepto de una red de datos neutral basada en el principio de "extremo a extremo", así como también el término de la neutralidad de la red en sí mismo, habían sido "cargados" al derecho de los

[254] Véase, Lemley Y Lessig, *supra* nota248; Wu, *supra* nota246.

[255] Lemley y Lessig, *supra* nota 248.

[256] *Ibíd*.

[257] Wu, *supra* nota 245246, en 145. Al prohibir la discriminación en la disposición de servicios de banda ancha y contenido, los entes reguladores podían garantizar que el "campo de juego" competitivo continuara nivelado o "meritocrático" para los desarrolladores de aplicaciones que quisieran acceder a esas redes, independientemente de quién las controlaba.

[258] En ese momento, Wu estaba menos preocupado por preservar la pureza arquitectónica de la internet abierta que por promover una forma de "competencia Darwiniana" donde "solamente sobrevive el mejor". Wu, *supra* nota246, en 142.

[259] No hay necesidad de ir más allá buscando evidencia, ya que las normas de internet abierta 2015 de la Comisión Federal de Comunicaciones adoptan precisamente el tipo de principio de la neutralidad de la red propuesto por Wu en 2003. Véase, Normas de internet abierta 2015, *supra* nota2.

derechos humanos y al discurso.[260] Si se la compara con la formación del derecho internacional en general, esta evolución ocurrió en un abrir y cerrar de ojos. Lo esencial para enmarcar este proceso fueron las declaraciones definitivas realizadas por los principales organismos de derechos humanos de las Naciones Unidas que confirmaron la convergencia de los derechos humanos y el mundo digital. Con especial énfasis, el Consejo de Derechos Humanos de las Naciones Unidas en junio de 2012 adoptó una resolución emblemática sobre "la promoción, la protección y el goce de los derechos humanos y la internet," que establecía que "los derechos que las personas tienen *fuera de línea* deben ser igualmente protegidos *en línea*, especialmente la libertad de expresión, aplicable independientemente de las fronteras y a través de cualquier medio que uno mismo elija".[261] Un año antes, en septiembre de 2011, el Comité de Derechos Humanos de las Naciones Unidas emitió y actualizó el artículo 19 de la Observación General sobre el Pacto Internacional de Derechos Civiles y Políticos, donde se establece en forma expresa que las protecciones estipuladas en el pacto tienen vigencia para todos los "modos de expresión basados en internet".[262] Si bien la resolución del Consejo de Derechos Humanos no tiene en sí misma fuerza normativa, goza de una importancia tal por ser una decisión unánime adoptada por la principal institución de derechos humanos de las Naciones Unidas no solo con el fin de reconocer esta convergencia sino para promoverla. Si bien con un perfil no tan elevado como el de la resolución del consejo, la observación

[260] *Véase*, por ejemplo, Belli, Luca, "End-to-End, Net Neutrality and Human Rights, in Net eutrality Compendium: Human Rights", *Free Competition and the Future of the Internet*, Luca Belli y Primavera De Filippi (eds.), Springer, No. 13, 2015, pp. 22-23.

[261] Consejo de Derechos Humanos de las Naciones Unidas, "The Promotion, Protection, and Enjoyment of Human Rights on the Internet", ¶ 1, U.N. Doc. A/HRC/20/L.13, 29 de junio de 2012, disponible en: http://bit.ly/2g667kw (con énfasis añadido). En una resolución anterior del 2011, el Consejo de Derechos Humanos había hecho referencia a la importancia de proteger los derechos a la libertad de expresión de los profesionales de los medios y del periodismo en internet como parte de una declaración más general sobre las libertades en los medios. Consejo de Derechos Humanos de las Naciones Unidas, "Information and Communications Technologies for Development", U.N. Doc. A/RES/66/184, 22 de diciembre de 2011. Al mismo tiempo, la gobernanza de internet y la importancia de las tecnologías digitales para el desarrollo han sido foco de atención de las Naciones Unidas, que lideraron el proceso de la Cumbre Mundial sobre la Sociedad de la Información y patrocinaron foros regulares sobre la gobernanza de internet. *Véase*, por ejemplo, Consejo de Derechos Humanos de las Naciones Unidas, "Freedom of Opinion and Expression", U.N. Doc. A/HRC/RES/12/16, 2 de octubre de 2009.

[262] Comité de Derechos Humanos de las Naciones Unidas, Observación General No. 34, ¶¶ 12, 15, 39, 43 & 44, U.N. Doc. CCPR/C/GC/34, 12 de septiembre de 2011 (de aquí en adelante la Observación General del Comité de Derechos Humanos 34).

general 34 revisada por el Comité de Derechos es, sin duda, el argumento con más peso, porque posee fuerza legal.[263]

Incluso ni la resolución del Consejo de Derechos Humanos ni la Observación General del Comité de Derechos Humanos menciona la neutralidad de la red *per se*. El primer reconocimiento oficial de la incorporación de la neutralidad de la red en el derecho internacional de los derechos humanos fue en junio de 2011, en la Declaración Conjunta sobre Libertad de Expresión e Internet emitida por el relator especial de las Naciones Unidas para la Libertad de Opinión y de Expresión; el representante para la Libertad de los Medios de Comunicación de la a Organización para la Seguridad y la Cooperación en Europa (OSCE); el relator especial para la Libertad de Expresión de la Organización de los Estados Americanos (OEA); y la relatora especial sobre la Libertad de Expresión y el Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP) (de aquí en adelante "Declaración Conjunta").[264] Entre los principios definidos en la Declaración Conjunta se encuentra el imperativo lacónico que dispone que "no debería haber discriminación en el tratamiento de los datos y del tráfico de internet según el dispositivo, contenido, autor, origen o destino del contenido, servicio o aplicación".[265] No se da razón alguna que explique cómo y por qué este principio ahora es una norma de derechos humanos respecto de internet.[266] Recién, en diciembre de 2013, surgió un debate más intenso sobre la relación entre la neutralidad de la red y la libertad de expresión, cuando el relator especial de la Comisión Interamericana de Derechos Humanos publicó su informe titulado: "Libertad de expresión e internet".[267] Conforme

[263] Las interpretaciones del Comité sobre las disposiciones del Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por su sigla en inglés) son, conforme al mismo tratado, autoritativas, y como tal obligan a los Estados a cumplir. Pacto Internacional de Derechos Civiles y Políticos, art. 40, 16 de diciembre de 1966, 1976 U.N.T.S. 999 (de aquí en adelante ICCPR).

[264] Declaración Conjunta, *supra* nota10.

[265] *Ibíd*. 5(a).

[266] El preámbulo expresa que el tema de la Declaración Conjunta se "discutió (…) junto con el aporte del Artículo 19, "Global Campaign for Free Expression and the Centre for Law and Democracy". Lo que queda claro es que la neutralidad de la red ha figurado de manera prominente durante algunos años primero en el trabajo de defensa realizado por organizaciones no gubernamentales internacionales como el artículoe 19 y otras. *Véase*, por ejemplo, Belli, Luca, y De Filippi, Primavera, "The Value of Network Neutrality for the internet of Tomorrow: Report of the Dynamic Coalition on Network Neutrality 2", 2013; Belli, Luca, "Council of Europe Multi-Stakeholder Dialogue on Network Neutrality and Human Rights", ¶¶ 16-17, 2013, disponible en: http://bit.ly/2grppEk. Entonces, es justo asumir que este trabajo, así como la consulta específica con las ONG, dieron forma a la Declaración Conjunta.

[267] Botero, Catalina, relatora especial de la OEA para la Libertad de Expresión, Freedom of Expression and the Internet, 2014, disponible en: http://bit.ly/2fJpW3L (de aquí en adelante Informe de la Relatora Especial de la OEA).

a la Declaración Conjunta firmada, la relatora especial para la Libertad de Expresión de la OEA, Catalina Botero, expresó en su Informe de 2013 que "la neutralidad de la red es parte del diseño original de internet [y] es fundamental para garantizar la pluralidad y la diversidad del flujo de información".[268] Al interpretar la Convención Americana sobre Derechos Humanos, la relatora especial afirmó de manera categórica que el respeto por la neutralidad de la red "es condición necesaria para ejercer la libertad de expresión en internet con sujeción a los términos del artículo 13 [de la Convención]".[269] Resulta curioso que el relator especial de las Naciones Unidas en sus informes de 2011 sobre libertad de expresión e internet (uno para el Consejo de Derechos Humanos y el otro para la Asamblea General) no menciona, y mucho menos debate sobre la neutralidad de la red.[270] Asimismo, la relatora especial de la comisión africana, Faith Pansy Tiakula, aparentemente no abordó el tema en sus publicaciones posteriores o en su posición.[271]

Siguiendo la iniciativa de su contraparte de la OEA, el representante para la Libertad de Medios de Comunicación de la OSCE, Dunja Mijatović, continuó en la defensa de la neutralidad de la red como un principio fundamental de los derechos humanos. En junio de 2014, en respuesta a las normas propuestas por la Comisión Federal de Comunicaciones de los Estados para regular la neutralidad de la red, el representante de la OSCE publicó un informe donde cita la Declaración Conjunta que concluyó que "las normas propuestas por la Comisión Federal de Comunicaciones amenazan la libre circulación de información en internet y ponen en peligro la libertad de expresión y la libertad de los valores de los medios".[272] En su presentación del informe, Mijatović

[268] *Ibíd*. ¶¶ 27-28.

[269] *Ibíd*. ¶ 25. El artículo 13 de la Convención Americana establece que "toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones". Convención Americana de los Derechos Humanos artículo 13, 22 de noviembre de 1969, 114 UNTS, pp. 148-49.

[270] *Véase*, *infra* notas 284-296 y texto acompañante.

[271] *Véase*, Comisión Africana para los Derechos Humanos y de los Pueblos, Relatora Especial sobre Libertad de Expresión y Acceso a la Información, disponible en: http://bit.ly/2f8wAez.

[272] Nunziato, Dawn C., OSCE, "The U.S. Federal Communications Commission's Proposed Rulemaking in the Matter of Protecting and Promoting the Open internet 3", 2014, disponible en: http://bit.ly/2fJqLcW.

expresó que "la internet fue concebida como un medio abierto siendo la libre circulación de información una de sus características esenciales… (…). Esto debería ser garantizado sin discriminación e independientemente del contenido, destino, autor, dispositivo usado u origen".[273]

Como mínimo, surge de lo antes explicado que el proceso de incorporar el principio de la neutralidad de la red en el discurso oficial de los derechos humanos a nivel mundial está en proceso.[274] No queda tan claro aún la cuestión técnica de cómo integrar este principio al marco del derecho internacional de los derechos humanos. Por cierto, en estos momentos resulta claro que "la finalidad de este principio es garantizar que el acceso libre y la elección del usuario de usar, enviar, recibir y ofrecer contenido, aplicaciones o servicios legales a través de internet no están [sic] sujetos a condiciones, pautados o restringidos como el bloqueo, el filtrado o la interferencia".[275] Esto fue una parte importante de lo que el Consejo y el Comité de Derechos Humanos de las Naciones Unidas pretendieron cubrir cuando afirmaron que el derecho de los derechos humanos se extiende al mundo digital si bien ninguno de ellos hizo referencia a la neutralidad de la red por su nombre. Pero ¿ese es el alcance de la convergencia de la neutralidad de la red y el derecho de los derechos humanos? ¿Qué otras dimensiones o ramificaciones existen donde se pueda incorporar la neutralidad de la red en el abanico de derechos a la libertad de expresión? ¿Existen otros derechos humanos que podrían estar involucrados? Pocos académicos y exponentes de la sociedad civil han comenzado a explorar las justificaciones legales que yacen detrás de la condición de la neutralidad de la red como norma de los derechos humanos.[276] Pero se necesita mucha más teoría en este sentido si se quieren garantizar los cimientos de la neutralidad de la red como norma de los derechos humanos.

[273] Comunicado de prensa, OSCE, "OSCE Representative Warns that U.S. Proposed Rules on Net Neutrality Can Hurt Online Media Freedom", 16 de junio de 2014, disponible en: http://bit.ly/2fp4ZXy.

[274] *Véase*, por ejemplo, Consejo de Europa, "Steering Committee on Media and Information Society, Protecting Human Rights through Network Neutrality Furthering internet Users' Interest, Modernizing Human Rights, and Safeguarding the Open internet", 3-6 de diciembre de 2013, disponible en: http://bit.ly/2gpVSsW. *Véase*, *además*, Informe de la Relatora Especial de la OEA, *supra* nota267. Por discurso "oficial" de los derechos humanos me refiero al que producen las organizaciones intergubernamentales de derechos humanos y sus expertos encargados de brindar interpretaciones acreditadas sobre el derecho internacional de los derechos humanos.

[275] Informe de la Relatora Especial de la OEA, *supra* nota267, en ¶ 25.

[276] *Véase*, por ejemplo, "The Value of Network Neutrality for the internet of Tomorrow: Report of the Dynamic Coalition on Network Neutrality", Luca Belli y Primavera De Fillippi (eds.), 2013, disponible en: http://bit.ly/2fY6Oi0. Informe de 2013 del CDT, *supra* nota26.

II.B. Neutralidad de la red y derecho de los derechos humanos contemporáneos

Los fundamentos del derecho de los derechos humanos que respaldan la norma de la neutralidad de la red no son completamente claros. En este sentido, intentaré esclarecer tres premisas en esta sección. Primero, con la descripción del marco del derecho internacional que regula la libertad de expresión y sus derechos inherentes, queda claro que la neutralidad de la red reacciona con mucho más que el derecho de brindar información o acceder a ella sin restricciones. En particular, el derecho de acceder a internet o a la "conectividad" es un imperativo normativo equivalente a la concreción de libertad de expresión. Segundo, para apreciar cómo opera la neutralidad de la red en carácter de garante de la libertad de expresión se necesita entender cómo las normas de la no discriminación incorporadas al derecho de los derechos humanos son receptores naturales de ese principio por separado. Tercero, independientemente de si uno prefiere ver la neutralidad de la red principalmente como función de expresión o como norma de no discriminación, es una norma de los derechos humanos que, como tal, está sujeta a las excepciones establecidas por el derecho internacional para determinar los límites permisibles que los Estados pueden imponer sobre los derechos fundamentales. Esto significa que, como todo derecho, no es absoluto.

Antes de pasar a esta discusión, es necesario recordar brevemente el alcance del deber que tiene el Estado de respetar y garantizar el respeto por los derechos humanos conforme al derecho internacional. Queda bien establecido que los Estados deben hacer tres cosas para cumplir con sus obligaciones en función de los derechos humanos. En primer lugar, deben actuar de buena fe para adoptar leyes y otras medidas requeridas para implementar aquellos derechos humanos que están obligados a respetar.[277] En segundo lugar, deben garantizar que sus agentes no violen los derechos

[277] *Véase*, Comité de Derechos Humanos, Observación General No. 31 Naturaleza de la obligación jurídica general impuesta a los Estados partes en el Pacto t, ¶ 3, U.N. Doc. CCPR/C/21/Rev.1/Add. 13, 26 de mayo de 2004 (de aquí en adelante HRC GC 31); *Véase*, Freedoms, artículo 1, *abierta para la firma*, 4 de noviembre de 1950, 213 U.N.T.S. 222 (de aquí en adelante Convención Europea sobre Derechos Humanos) (entró en vigor el 3 de septiembre de 1953); Organization of African Unity (Organización para la Unidad Africana), Carta Africana (Banjul) de los Derechos Humanos y de los Pueblos, artículo 1, *abierta para firma*, 27 de junio de 1981, 1520 U.N.T.S. 123 (de aquí en adelante Carta de Banjul de los Derechos Humanos) (entró en vigor el 21 de octubre de 1986); Organización de los Estados Americanos, Convención Americana de Derechos Humanos, artículo 1, 22 de noviembre de 1969, OASTS No. 36, 1.144 U.N.T.S. 123 (entró en vigor el 18 de julio de 1978).

humanos directamente a través de acciones u omisiones, y si lo hicieran, brindar las soluciones efectivas y apropiadas para las víctimas con el fin de subsanar esas transgresiones.[278] En tercer lugar, los Estados tienen el deber afirmativo de garantizar el goce de los derechos humanos a todas las personas en su territorio o bajo su jurisdicción, lo cual significa que deben actuar de manera inteligente para impedir abusos por terceros, y brindar las soluciones apropiadas y eficaces frente a casos de abuso por actores privados.[279] En cuanto a este último aspecto:

> Las obligaciones positivas de los Estados (…) para garantizar los derechos [humanos] serán cumplidas en su totalidad cuando las personas estén protegidas por el Estado, no solo contra violaciones de [esos] derechos por sus agentes sino también contra actos cometidos por personas o entidades privadas que impedirían el goce de [esos] derechos siempre que pueden considerarse personas o entidades privadas. Puede haber casos donde la falta de garantía de los derechos [humanos] conforme al derecho internacional daría lugar a violaciones… de aquellos derechos por parte de los Estados, debido a… la falta de adopción de medidas pertinentes o del ejercicio de la debida diligencia para impedir, sancionar, investigar o subsanar el daño que provocan dichos actos por parte de personas o entidades privadas.[280]

II.B.I. Libertad de expresión en el derecho internacional

Pocos derechos son definidos con la particularidad de la libertad de expresión. El artículo 19 del ICCPR, por ejemplo, afirma que "la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o

[278] *Ibíd*., HRC GC 31, en ¶¶ 8, 15; *Ibíd*., Convención Europea sobre Derechos Humanos, artículo 13; *Ibíd*., Convención Americana de Derechos Humanos, art. 25.

[279] Véase, por ejemplo, HRC GC 31,. Este deber afirmativo conforme a los derechos humanos internacionales se contrapone drásticamente con el deber negativo principal impuesto sobre los actores gubernamentales por la Primera Enmienda de los Estados Unidos. Véase, Nunziato, Dawn C., "Virtual Freedom: Net Neutrality and Free Speech in the Internet Age", Stanford Law Books, California, 2009.

[280] HRC GC 31, *supra* nota277, en ¶ 8; *Véase* además, Application of Convention on Prevention and Punishment of Crime of Genocide ("Bosnia y Herzegovina vs. Serbia y Montenegro"), sentencia, 2007 Corte Internacional de Justicia 43, ¶¶ 166, 430 (resolvió que existe una obligación de diligencia debida para los Estados "de usar los medios que estén a su alcance… para impedir que personas o grupos que no estén directamente bajo su autoridad cometan" actos de genocidio, ¶166).

artística, o por cualquier otro procedimiento de su elección".[281] Este lenguaje refleja el artículo 19 de la Declaración Universal de Derechos Humanos"[282] (de aquí en adelante "DUDH"). Podemos encontrar un lenguaje bastante similar en el artículo 10 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, y en el artículo 13 de la Convención Americana de Derechos Humanos.[283] Asimismo, muchas, por no decir la mayoría de las naciones del mundo, han adoptado normas para proteger el libre discurso y la libertad de expresión en sus constituciones.[284] La libertad de expresión goza de aceptación casi universal, particularmente debido a que se la percibe correctamente como facilitador de otros derechos humanos básicos. Los derechos humanos incluyen no solamente los derechos corolarios de tener opiniones o creencias religiosas sin interferencia alguna, sino también otros como el derecho a la educación, el derecho a la libertad de reunión y de asociación, el derecho a participar plenamente en la vida social, cultural y política y el derecho al desarrollo social y económico.[285]

Tradicionalmente, la libertad de expresión se ha dividido en varios componentes, a saber: (1) el derecho a ofrecer o expresar información e ideas en general; (2) el derecho de los medios; (3) el derecho a buscar y recibir información e ideas en general; y (4) el derecho de acceder a la información "de las entidades públicas".[286] En particular, cabe destacar la importancia del pluralismo de medios, que los Estados están obligados a promover mediante "la acción apropiada (…) para impedir la dominación o concentración indebida de los medios por grupos de medios controlados en forma privada en situaciones monopólicas que podrían ser perjudiciales para una diversidad de fuentes y opiniones".[287]

---

[281] ICCPR, *supra* nota263, artículo 19 (2).

[282] G.A. Res. 217 (III) A, Declaración Universal de los Derechos Humanos, en 19, 10 de diciembre de 1948.

[283] Convención Europea sobre Derechos Humanos, *supra* nota 277, art. 10; Convención Americana de Derechos Humanos, *supra* nota 277, artículo 13.

[284] *Véase*, por ejemplo, Toby Mendel et al., "Global Survey on internet Privacy and Freedom of Expression", UNESCO Series on internet Freedom, 2012.

[285] La Rue, Frank, Naciones Unidas Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression ¶ 61, U.N. Doc. A/66/290, 10 de agosto de 2011, (de aquí en adelante Informe SR GA 2011).

[286] Comité de Derechos Humanos, "Observación General No. 34: Artículo 19 (Libertad de opinión y Libertad de expresión)", ¶¶ 11, 18, U.N. Doc. CCPR/C/GC/34, 12 de septiembre de 2011, (de aquí en adelante HRC GC 34). Cada uno se describe más exhaustivamente en la Observación General Nº 34. Los derechos de los medios, por ejemplo, se describen en detalle en ¶¶ 13-17, pp. 37-42.

[287] *Ibíd*. ¶ 40.

Desde la aparición de las comunicaciones electrónicas, el marco precedente de la libertad de expresión ha evolucionado para admitir la transmisión y recepción de información e ideas por medio de internet. Como se observó en la subsección anterior, ha quedado establecido que los derechos que comprenden la libertad de expresión se aplicarán en la actualidad a todas las "formas de comunicación basadas en internet".[288] Como materia práctica esto significa que "toda restricción sobre el funcionamiento de los sitios web, blogs u otro sistema basado en internet, electrónico o de otro tipo, a los fines de diseminar información, incluso los sistemas para respaldar esas comunicaciones, como los proveedores de servicios de internet o los motores de búsqueda solo son permisibles hasta el punto tal que sean compatibles con el párrafo 3 [del artículo 19]".[289] Más adelante analizaré el régimen de excepciones.

Resulta igualmente útil recordar aquí que el régimen de responsabilidad del Estado resumido al inicio de esta sección específicamente "requiere que los Estados garanticen que las personas estén protegidas contra actos realizados por personas o entidades privadas que impedirían el goce de la libertad de opinión y de expresión hasta el punto que esos derechos estén sujetos a aplicación entre personas o entidades privadas".[290] Los Estados tienen el deber afirmativo, por ende, de adoptar medidas y actuar en forma diligente para garantizar que los derechos de la libertad de expresión sean protegidos contra conductas perpetradas por actores privados que pudieran vulnerar el goce de esos derechos por los demás.[291]

Para completar el abanico de los derechos de la libertad de expresión relacionados con la neutralidad de la red, tenemos la dimensión más reciente del derecho de acceder a la información: la conectividad.[292] En palabras simples: "La implementación del derecho a la libertad de expresión impone a los Estados la obligación de promover el acceso universal a internet".[293] Esta obligación positiva significa que para que los Estados puedan cumplir con su deber de respetar y cumplimentar con el derecho a la libertad de

[288] *Ibíd*. ¶ 12.

[289] *Ibíd*. ¶ 43.

[290] *Ibíd*. ¶ 7.

[291] *Véase*, *supra* notas 283-284 y texto acompañante.

[292] No parece existir una definición de conectividad aceptada universalmente en el derecho internacional o en la práctica. La "conectividad" se entiende aquí como el acceso a todo tipo de conexión a internet que brinda acceso parcial o completo a servicios, aplicaciones e información disponible en línea.

[293] Declaración Conjunta, *supra* nota10, en 3; *véase además*, Res. 20/8 Consejo de Derechos Humanos, ¶ 3, U.N. Doc. A/HRC/20/L.13, 29 de junio de 2012.

expresión, deben garantizar que todas las personas dentro de su territorio tengan acceso a "los medios necesarios para ejercer ese derecho, lo que [hoy en día] incluye internet".[294] Por consiguiente, el Comité de Derechos Humanos ha instado a los Estados a "adoptar las medidas necesarias para promover la independencia de (…) los nuevos medios (…) como internet y los sistemas móviles de diseminación de información electrónica, *y asegurar el acceso de todos los individuos*".[295] La conectividad es, por ende, "esencial" para concretar la libertad de expresión.[296]

El deber de la buena fe que pesa sobre los Estados para trabajar de manera diligente hacia la implementación efectiva de la libertad de expresión tiene una relevancia similar a la de concretar en forma progresiva otro derecho fundamental, como el derecho a la educación, a la salud, al desarrollo socioeconómico, y a la participación política.[297] Por esas razones los grandes expertos de los cuatro sistemas jurídicos más importantes recalcaron en 2011 que, como mínimo, los Estados deben "implementar mecanismos regulatorios –como por ejemplo regímenes de fijación de precios, requisitos de servicios universales y contratos de licencia– que fomenten un mayor acceso a internet, incluso para las zonas pobres y rurales "rezagadas".[298] En los tiempos modernos, es difícil exagerar el rol transcendental de la conectividad como parte integral de la libertad de expresión en la concreción de los derechos humanos en general.

II.B.II. No discriminación en el derecho internacional

La no discriminación es un principio de primer orden del derecho internacional de los derechos humanos. "La no discriminación junto con la igualdad ante la ley y la protección igualitaria de la ley sin discriminación, constituyen el principio básico y general en términos de protección de los

[294] *Véase*, Informe SR GA 2011, *supra* nota 286, Parte III. *Véase*, Informe SR GA 2011, *supra* nota 286 ¶ 61.

[295] HRC GC 34, *supra* nota 287, ¶ 15 (con énfasis añadido); véase además, Informe de la Relator Especial de la OEA, *supra* nota 267, ¶ 11 ("Es importante que todas las regulaciones se basen en el diálogo entre todos los actores y mantener las características básicas del entorno original, fortaleciendo la capacidad democratizadora de internet y promoviendo el acceso universal y no discriminatorio").

[296] *Véase*, Informe SR GA 2011, *supra* nota 286, ¶ 61.

[297] Res. 20/8 Consejo de los Derechos Humanos, ¶ 3, U.N. Doc. A/HRC/20/L.13, 29 de junio de 2012; *Véase*, además, *infra* notas 318-331 y texto acompañante. Sobre el deber de los Estados de implementar sus obligaciones respecto de los derechos humanos básicos, *véase*, por ejemplo, ICCPR, *supra* nota 263, en artículo 2(2).

[298] Declaración Conjunta, *supra* nota 10, ¶ 6(e)(i).

derechos humanos".[299] Por esa razón, una vez más copiando la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos establece que los Estados están obligados a "respetar y garantizar para todos los individuos dentro de [su] territorio y sujeto a [su] jurisdicción, los derechos [humanos] reconocidos (…) sin distinción de todo tipo, raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o extranjero, posición económica, nacimiento o cualquier otra condición".[300] Al mismo tiempo, "todos son iguales ante la ley y tienen, sin distinción, derecho a igual protección por parte de la ley".[301] Esta disposición prohíbe "la discriminación conforme a la ley y garantiza a todas las personas igual protección efectiva contra la discriminación de cualquier tipo", o según todo tipo de distinción en base a los enumerados anteriormente.[302] Principios antidiscriminatorios muy similares a estos aparecen en todos los tratados de derechos humanos a nivel mundial o local.[303] Entonces, en la medida en que la neutralidad de la red sea mejor entendida como un principio de no discriminación aplicado a los derechos de los usuarios de solicitar, recibir o impartir datos o información en línea encuadra de manera orgánica con las normas centrales de la no discriminación del derecho internacional de los derechos humanos.

La discriminación ilícita de cualquier tipo es la negación de la igualdad y la dignidad humana. Según el derecho internacional de los derechos humanos, la discriminación es "toda distinción, exclusión, restricción o preferencia basada en raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o *cualquier otra condición,* con la finalidad de anular o impedir el reconocimiento, el goce y el ejercicio de los derechos y las libertades para todos en iguales condiciones".[304] Pero no toda la discriminación es ilegal *per se*. El derecho internacional hace una distinción entre discriminación negativa y positiva. El "principio de la igualdad algunas veces requiere que los

[299] Comité de los Derechos Humanos, "Observación General No. 18 sobre la no discriminación (Sesión trigésima séptima, 1989)", Compilación de observaciones generales y recomendaciones generales adoptadas por los organismos sobre derechos humanos, U.N. Doc. HRI/GEN/1/Rev.1, 29 de julio de 1994, en 26 (de aquí en adelante HRC GC 18).

[300] *Íbíd*., ¶ 1; *véase además*, ICCPR, *supra* nota 263, en artículo 2.

[301] ICCPR, *supra* nota 263, en artículo 26.

[302] HRC GC 18, supra nota 300, ¶ 1.

[303] *Véase*, por ejemplo, Convención Europea sobre Derechos Humanos, *supra* nota 277, artículo 14; Carta de los Derechos Humanos de Banjul, *supra* nota 275, art. 2; Convención Americana de Derechos Humanos, *supra* nota 277, art. 24.

[304] HRC GC 18, *supra* nota 300, ¶ 7 (con énfasis añadido).

Estados parte adopten acciones afirmativas con el fin de disminuir o eliminar condiciones que causan o conducen a perpetuar la discriminación prohibida [por el Derecho Internacional]".[305] Debido a ello, "no toda diferencia en el tratamiento constituye discriminación [ilegal], si los criterios para dicha diferenciación son razonables y objetivos, y si la finalidad es lograr un fin que sea legítimo conforme al [derecho internacional]".[306]

La pregunta pendiente es qué cuenta como "otra condición" a los fines de determinar qué distinciones adicionales podrían llevar a una discriminación negativa (o positiva). Es importante destacar que el derecho internacional de los derechos humanos reconoce distinciones basadas en la condición o el criterio *económico*, y evalúa si la finalidad o el *efecto* se proponen anular u obstaculizar el ejercicio o el goce de otros derechos humanos.[307] Por ende, por ejemplo, el Comité de los Derechos Humanos de las Naciones Unidas decidió que, en Islandia, la diferencia legal entre dos grupos de pescadores, donde uno fue forzado a pagar aranceles exorbitantes para pescar, al otro grupo a quien el Estado le había otorgado licencias permanentes, exclusivas con cupos por razones históricas, constituye una distinción ilegal basada en privilegios no razonables de "derecho a la propiedad".[308] Por otro lado, como se explicó anteriormente, cuando dicha distinción se basa en criterios "razonables y objetivos" y pretende promover un propósito válido del Estado, puede considerarse que refleja una "diferencia legítima" conforme al derecho internacional.[309] Por consiguiente, por ejemplo, un Estado podría implementar una reducción impositiva temporaria para los trabajadores con ingresos bajos en un sector crítico pero deprimido de la economía, es decir, la construcción.[310] Incluso aunque las medidas discriminarían a trabajadores en igual situación en otros sectores que no recibieran reducciones impositivas, el Estado estaría persiguiendo, si bien es discutible, un objetivo legítimo (para mejorar un sector importante de su economía y promover derechos socio-económicos) mediante

[305] *Ibíd*. ¶

[306] *Ibíd*. ¶ 13.

[307] *Véase*, "Haraldsson vs. Islandia, Comunicación", No. 1306/2004, Opinión del Comité, Consejo de los Derechos Humanos de las Naciones Unidas, ¶ 10.3, 24 de octubre de 2007, disponible en: http://bit.ly/2gq5q7i.

[308] *Ibíd*. ¶¶ 10.3-10.4 ("El Comité concluye que el privilegio del derecho a la propiedad acordado en forma permanente a los titulares originales de los cupos [de pesca], en detrimento del [otro pescador], se basa en fundamentos razonables").

[309] *Véase*, *supra* notas 306-307 y texto acompañante.

[310] *Véase*, por ejemplo, RPCWM, "Brandsma vs. Holanda", Comunicado No. 977/2001, decisión de admisibilidad, Comité de Derechos Humanos de las Naciones Unidas, ¶¶ 6.3-6.4, 1 de abril de 2004, disponible en: http://bit.ly/2gPFP4v.

criterios objetivos (concentrándose en los trabajadores con ingresos bajos y de un sector deprimido) para adoptar medidas razonables (reducciones impositivas con duración limitada) con el fin de lograr ese objetivo[311]. Dicha política no violaría probablemente las obligaciones de no discriminación impuestas por el derecho internacional de los derechos humanos.

II.B.III. El régimen de excepciones para la libertad de expresión

Las normas de derechos humanos en general, y la libertad de expresión en particular, no son absolutas.[312] El derecho de los derechos humanos permite de forma expresa ciertas restricciones sobre el derecho a la libertad de expresión que "respeta […] los derechos o las reputaciones de otros" o promueve "la protección de la seguridad nacional, o el orden público […], o la salud pública o la moral".[313] Estos son, en términos generales, objetivos legítimos que justificarán la acción del Estado cuando actúa para restringir derechos humanos fundamentales como la expresión[314]. Pero por supuesto, puede haber otros. Observamos cómo los Estados pueden en circunstancias limitadas aplicar la discriminación positiva para abordar consecuencias sociales o de otro tipo de discriminación ingrata anterior.[315] Además de perseguir un objetivo legítimo, el Estado que busca limitar la libertad de expresión debe garantizar que toda restricción sea "establecida por la ley", "necesaria" para cumplir con ese objetivo y "proporcional".[316] La existencia del régimen de excepciones, sin

[311] *Ibíd*. El Comité de Derechos Humanos no resolvió el caso por el fondo de la causa, decidió que era inadmisible por falta de evidencia que los regímenes de pagos impositivos en cuestión fuesen sustancialmente comparables. Sin embargo, el debate en el Comité sobre los temas subyacentes sugiere que podría quizás haber decidido que dicho régimen servía a los fines de promover el objetivo legítimo del Estado de una manera permisible.

[312] Un buen ejemplo es el ICCPR, *supra* nota 262, en art. 20, que enumera de manera explícita una serie de formas de expresión ofensivas que los Estados *deben* restringir con el fin de cumplir con sus obligaciones conforme al tratado. ("1. Toda propaganda en favor de la guerra estará prohibida por la ley. 2. Toda apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia estará prohibida por la ley").

[313] ICCPR, *supra* nota 263, en artículo 19(3); HRC GC 34, *supra* nota 287, en ¶¶ 28-32.

[314] *Véase*, La Rue, Frank, relator especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Consejo de los Derechos Humanos, U.N. Doc. A/HRC/23/40, 17 de abril de 2013, ¶ 28 ("El marco del artículo 17 del ICCPR permite restricciones necesarias, legítimas y proporcionales al derecho de privacidad por medio de limitaciones permisibles").

[315] *Véase*, *supra* notas 305-306 y texto acompañante.

[316] ICCPR, *supra* nota 263, en artículo 19(3); HRC GC 34, *supra* nota 287, en ¶¶ 24-26, 33-34; Informe SR GA 2011, *supra* nota 286, ¶ 15.

embargo, no es un cheque en blanco: "Cuando un Estado impone restricciones en el ejercicio de la libertad de expresión, esto no podría poner en riesgo el derecho en sí mismo".[317] En otras palabras, las excepciones deben seguir siendo una excepción y no pueden convertirse en una regla.[318]

Cada elemento del marco de las excepciones amerita una explicación más detallada. Los objetivos legítimos que los Estados pueden perseguir, están estipulados en el derecho internacional.[319] Aquí, cabe destacar el objetivo de proteger y promover *los derechos de otras personas* como base para restringir una norma en particular. Las leyes sobre la difamación son ejemplos clásicos de límites severos impuestos sobre la libertad de expresión para proteger la reputación de otros.[320] Y así como "una diferencia legítima" a favor de los grupos que siempre han estado en desventaja puede promover de manera afirmativa los objetivos de la no discriminación,[321] de esa misma forma la restricción de los derechos de la libertad de expresión puede servir para fomentar los derechos de la libre expresión de otros.[322] Por ende, por ejemplo, "está permitido proteger a los votantes [que desean expresar su opinión política] contra formas de expresión que constituyan intimidación o coerción".[323] En la práctica, los Estados tienen generalmente un cierto margen para determinar qué políticas adoptarán con el fin de promover

[317] HRC GC 34, *supra* nota 287, en ¶ 21.

[318] "La relación entre el derecho y la restricción entre la norma y la excepción no debe ser revocada".

[319] ICCPR, *supra* nota 263, en artículos 19, 20.

[320] HRC GC 34, *supra* nota 287, en párr. 47 ("Las leyes sobre difamación deben redactarse con cuidado para asegurarse de que cumplan lo dispuesto en el párrafo 3 y no sirvan en la práctica para atentar contra la libertad de expresión").

[321] *Supra* nota 310 texto acompañante.

[322] R GC 34, *supra* nota 287, en párr. 28 ("El término 'derechos' comprende los derechos humanos reconocidos en el Pacto y, más en general, en la normativa internacional de los derechos humanos (…). La expresión 'los demás' puede referirse a otras personas a título individual o como miembros de una comunidad").

[323] *Ibíd*. Es claro que esto implica el derecho distintivo a voto del artículo 25, sin quitarle relevancia a la expresión política que se concreta a través del voto. *Véase*, "Vladimir Viktorovich Shchetko vs. Bielorrusia", Comunicado No. 1009/2001, U.N. Doc. CCPR/C/87/D/1009/2001, 2006), disponible en: http://bit.ly/2fxtaDj en ¶ 7.4 ("El Comité recuerda que conforme al artículo 25(b), cada ciudadano tiene derecho a voto, y para proteger ese derecho, los Estados parte del Pacto deberían prohibir todo tipo de intimidación o coerción hacia los votantes por medio de leyes penales y que dichas leyes deberían ser aplicadas con fuerza [4]. La aplicación de dichas leyes constituye, en principio, una limitación legal del derecho a la libertad de expresión, necesaria para respetar los derechos de los demás"); "Leonid Svetik vs. Bielorrusia", Comunicado No. 927/2000, U.N. Doc. CCPR/C/81/D/927/2000, 2004, disponible en: hhttp://bit.ly/1jAPl8F en ¶ 7.3 (establece la misma propuesta).

o cumplir con objetivos específicos dentro de la categoría general de los objetivos legítimos identificados.[324]

Si asumimos que la finalidad de un Estado es promover un objetivo legítimo reconocido por el derecho internacional, toda restricción propuesta sobre la libertad de expresión no debe solamente estar establecida por ley, sino que debe ser necesaria y proporcional. Esto significa colocar una vara alta para reconocer un pequeño conjunto de medidas estrictamente diseñadas.[325] En términos generales, dichas restricciones deberían ser sancionadas en leyes formales a través de un proceso político transparente y participativo.[326] En todo caso, dichas leyes "deben ser formuladas con la precisión suficiente para permitir que el individuo regule su propia conducta de conformidad"[327]. Asimismo, deben ser accesibles al público.[328] A fin de ser "necesarias", los límites sancionados legalmente deben estar "directamente relacionados para [cumplir] la necesidad específica que afirman",[329] es decir, deben ser efectivos en cuanto al fin para el cual fueron establecidos. La imposición de una restricción no es indispensable y por lo tanto "viola la prueba de necesidad [,] si la protección pudiera lograrse de otra forma que no restringiera la libertad de expresión".[330] Por último, todas las acciones adoptadas por los Estados para limitar la expresión, incluso si fuesen legítimas y necesarias, no pueden ser "exageradas".[331] Las medidas proporcionales son aquellas que resultan "apropiadas para lograr su función protectora" e "intrusivas al

[324] *Véase*, "Leo Hertzberg et al. vs. Finlandia", Comunicado No. 61/1979 U.N. Doc. CCPR/C/OP/1, 1985, disponible en: http://bit.ly/2gq7EU9 (reconoce que "debe acordarse un cierto margen de discreción para las autoridades responsables a nivel nacional" cuando deciden si transmiten debates relacionados con relaciones homosexuales a través de los medios nacionales); *Véase*, además, Schmidt, Markus, "Book Review", 10 Harvard Human Rights. J. 313, 338, 1997 (interpreta las decisiones de la Comisión de Derechos Humanos basándose en el margen de razón de la apreciación); *Véase*, además, Legg, Andrew, "The Margin of Appreciation in International human Rights Law: Deference and Proportionality 41", Oxford, 2012 ("No hay casos claros en la Corte Interamericana de Derechos Humanos [IACtHR] y en el Comité de Derechos Humanos de las Naciones Unidas (UN HRC) que rechazan el margen de apreciación como resultado del relativismo sobre los derechos humanos").

[325] *Véase*, HRC GC 34, *supra* nota 287, en párr. 35.

[326] *Véase*, relator especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Consejo de Derechos Humanos, U.N. Doc. A/HRC/17/27, 16 de mayo de 2011, (por Frank La Rue), ¶ 24.

[327] HRC GC 34, *supra* nota 287, ¶ 25.

[328] *Ibíd*.

[329] *Ibíd*. en ¶ 22.

[330] *Ibíd*. en ¶ 33.

[331] *Ibíd*. en ¶ 34

mínimo nivel entre aquellas medidas [disponibles]".[332]

En síntesis, las subsecciones que anteceden han aclarado las razones técnicas por las cuales la incorporación formal de la neutralidad de la red en el derecho internacional como norma de derechos humanos es una premisa. En particular, he demostrado que la libertad de expresión está compuesta por varias normas, algunas de las cuales reaccionan frente a la neutralidad de la red. Sumado al derecho "clásico" de impartir o acceder a la información, el derecho de acceso a internet –la conectividad– es esencial para la plena concreción del derecho de expresión en la actualidad. Asimismo, expliqué cómo los principios de no discriminación incluidos en el derecho de los derechos humanos interactúan con la libertad de expresión, y por qué son receptores naturales de la neutralidad de la red. Finalmente, describí el marco que gobierna cuándo y cómo los Estados pueden sancionar excepciones legítimas para la libertad de expresión y las normas de no discriminación. Esta descripción del régimen de excepciones conforme al derecho internacional explica por qué ni la libertad de expresión ni las normas de no discriminación están exentas en su totalidad de las restricciones impuestas por el Estado que promueven los objetivos legítimos del mismo, como la promoción y protección de los derechos de los demás. Cualquiera de esos límites, no solo debe estar prescripto en forma de ley, sino que debe probarse como necesario y hecho a medida para lograr los fines legítimos identificados.

II.C. ¿Por qué el derecho internacional de los derechos humanos?

¿Por qué importa que la neutralidad de la red sea hoy en día una norma consolidada del derecho internacional de los derechos humanos? Con pocas excepciones, la mayoría de los debates de la actualidad sobre *zero-rating* se han concentrado en las implicancias económicas, sociales y técnicas de permitir o prohibir dichas prácticas en un determinado país.[333] Si bien se ha prestado un poco de atención a la neutralidad de la red como norma que promociona y protege los derechos humanos,[334] esta perspectiva no ha sido aún extendida por completo al *zero-rating*. Como resulta evidente, volver a enmarcar la neutralidad de la red y el *zero-rating* como cuestiones de derechos humanos nos conduce a una serie de consecuencias significativas.

Existen ventajas sustantivas y estratégicas para invocar el marco legal de los derechos humanos. Primero, de conformidad con el derecho de los

[332] *Ibíd*. en ¶ 34.

[333] *Véase*, *supra* nota 24 y texto acompañante.

[334] *Véase*, por ejemplo, Informe CDT de 2013, *supra* nota 26 e Informe EC Luca Belli EC, *supra* nota 276 y texto acompañante.

derechos humanos, la neutralidad de la red está definida como término centrado en la esfera humana en lugar de la esfera de los datos.[335] Este cambio no es tan solo semántico, ya que supone consecuencias importantes para la implementación de la norma, especialmente en cuanto a la conectividad. En especial, significa que las prácticas de *zero-rating* como transgresiones de la neutralidad de la red ya no pueden ser debatidas en términos de todo o nada. En su lugar, estas prácticas tienen que considerarse como límites sobre la libertad de expresión de *algunas* personas (entendidas como neutralidad de la red), que en gran parte pretenden ampliar los derechos de la libertad de expresión de los demás (es decir, a través del acceso expandido). En segundo lugar, como se explicó en la sección anterior, este nuevo marco coloca las cuestiones de la neutralidad de la red directamente dentro del marco normativo universalmente reconocido que impone obligaciones legales claras en la mayoría de los Estados.[336] La protección de la neutralidad de la red entonces se convierte en un deber que incumbe a los gobiernos, en lugar de ser una alternativa de política, obligatoria o polémica. Esto garantiza que las discusiones sobre cómo limitar la neutralidad de la red, como las ocurridas en los Estados Unidos, Europa, México y muchos otros países, se dan dentro del mismo régimen aplicado universalmente y establecido por el derecho internacional, promoviendo una mayor consistencia en la normativa.[337]

Por último, pero no menos importante, en base a todas las razones antes expuestas, el marco de los derechos humanos proporciona estructura y rigor a los debates polémicos y frecuentes sobre un dogma sin fundamentos: el absolutismo de la neutralidad de la red que choca con la inviolabilidad del mercado. Evaluar la regulación de la neutralidad de la red como función de las obligaciones del Estado conforme al derecho internacional abre una puerta práctica para el debate constructivo del *zero-rating*, porque establece parámetros normativos que se aplican por igual a todas las partes involucradas en los debates. Las personas dejaron de hablar *del* otro y comenzaron a hablar unos *con* otros. Al mismo tiempo –y esto es de vital importancia– el

[335] *Véase*, *supra* notas 281-284 y texto acompañante.

[336] El ICCPR tiene 168 Estados parte, conforman casi el 85% de la población mundial. *Véase* Colección de Tratados de las Naciones Unidas, Capítulo IV Derechos Humanos, 4. Pacto Internacional de Derechos Civiles y Políticos, disponible en: http://bit.ly/1j60Nly. Asimismo, la Declaración Universal de Derechos Humanos es considerada una fuente del derecho internacional consuetudinario, que cubriría al resto de los Estados miembro de las Naciones Unidas de una manera bastante similar. *Véase*, por ejemplo, Oficina del Alto Comisionado para los Derechos Humanos (Digital Record of the UDHR), febrero de 2009, disponible en: http://bit.ly/2fjQUwY.

[337] El Consejo Europeo ha adoptado este enfoque. *Véase*, McCarthy, *supra* nota 21.

enfoque de los derechos humanos es el único que representa de manera expresa a todos los demás. Aquellas personas que consideran la neutralidad de la red como un principio sagrado pondrán poca atención a lo que los economistas y defensores del libre mercado digan; otros que critican la neutralidad de la red como una preferencia de prioridad maleable podrán priorizar la competencia, el gusto del consumidor o el interés público. En otras palabras, las perspectivas dominantes –social, económica, técnica– que caracterizan los debates de la neutralidad de la red y el *zero-rating* no se adaptan fácilmente una a la otra, cuando lo hacen. Muy pocas personas realmente hacen referencia directa a los derechos humanos.

El derecho de los derechos humanos es diferente: es la unificadora "teoría del todo". Todos los demás enfoques tienen un lugar en el marco normativo como *aportes* cuantitativos y cualitativos para el análisis de las obligaciones del Estado sobre la promoción y protección de los derechos de sus ciudadanos. Los datos que revelan si las prácticas *zero-rating* promueven u obstaculizan el acceso a internet de manera significativa o no, integran el análisis de la *necesidad* de las medidas propuestas. Los estudios de mercado sobre el impacto de las prácticas *zero-rating* sobre la innovación, la competencia y la experiencia del usuario formarán parte del análisis para determinar si las prácticas *zero-rating* autorizadas son *proporcionales*. Las cuestiones sobre políticas se incluyen en la discusión sobre qué constituye un objetivo legítimo para aquellos Estados que buscan restringir la libertad de expresión imponiendo límites a la neutralidad de la red a través de la fijación de precios diferenciales (u otros medios). Tal como analizaré en la parte final, tanto si uno evalúa la legitimidad de los objetivos del Estado o la naturaleza de la fijación de precios diferenciales y su impacto sobre la neutralidad de la red, todos los datos relevantes –sociales, económicos, políticos, técnicos– jugarán un rol y se los ponderará frente a factores compensatorios reconocidos por el marco de los derechos humanos. No es posible decir lo mismo de otros enfoques.

III. Hacia un análisis del *zero-rating* desde la perspectiva de los derechos humanos

Los derechos humanos pueden ser invocados por defensores de todas las perspectivas generadas en los debates sobre la neutralidad de la red y *zero-rating*. Aquellos que defienden el concepto esencialmente no calificado de la neutralidad de la red insisten en que los derechos de las personas de recibir o impartir información e ideas libremente deberían rara vez, si es

que ocurre, verse perjudicados (si bien la mayoría admite la necesidad de algunas excepciones, por ejemplo, administrar de manera razonable la red o proteger su integridad). Creen que mantener una prohibición casi general sobre la diferenciación en el manejo del tráfico de internet, y preservar la pureza del principio de "extremo a extremo", es la mejor –o la única– forma de preservar verdaderamente la integridad y el potencial ilimitado de la red.[338] Por esas razones, entre otras, prefieren buscar alternativas al *zero-rating* en el mundo en vías de desarrollo que puedan promover el objetivo loable de aumentar la conectividad total sin sacrificar la neutralidad de la red. Los defensores de las prácticas *zero-rating*, por otro lado, justifican de manera frecuente su postura al apuntar a la sorprendente brecha digital y al imperativo de empoderar a las masas de personas desconectadas que viven en su mayoría en países en vías de desarrollo por cualquier medio disponible. En esta perspectiva más pragmática, el fin justifica los medios: la mejor manera de mejorar la situación de aquellas personas sin derecho, es garantizar, según dicen, el derecho al acceso por lo menos a internet en primer lugar, como un trampolín hacia un mayor acceso, que permita entonces ejercer su derecho de expresión y gozar de los beneficios de otros derechos humanos también, incluso si eso significa restringir la neutralidad de la red a través del *zero-rating.*[339]

Como regla, cuando los defensores de ambas perspectivas hacen una referencia expresa a los derechos humanos para respaldar sus argumentos, esas referencias tienden a ser como mucho superficiales. Incluso cuando los defensores de los derechos digitales invocan los derechos humanos de manera más formal, el análisis adicional es incompleto o deficiente. Este artículo ha abordado esas lagunas normativas mediante la explicación del funcionamiento del marco jurídico aplicable de los derechos humanos, ese fue el objeto de la Parte II. En esta última parte, considero ese marco en contexto con referencia a los datos empíricos presentados en la Parte I. En particular, analizo los elementos principales del régimen de excepciones –objetivo legítimo, necesidad y proporcionalidad– para ilustrar mejor cómo se

[338] *Véase*, por ejemplo, Crawford, Susan, "Zero for Conduct", Backchannel, disponible en: http://bit.ly/2gPGmnn ("El objetivo de la neutralidad de la red es preservar la internet como el camino abierto fundamental para la comunicación en que ha llegado a convertirse. La razón de que los gobiernos de China, Rusia y Cuba temen abrir la internet se debe especialmente a que le permite a los usuarios reunirse y hablar con otros […] Las relaciones y el desarrollo son los atributos fundamentales de internet - la innovación y el discurso libre - y eso no debe ser transgredido").

[339] *Véase*, por ejemplo, Hempel, Jessi, "Inside Facebook's Ambitious Plan to Connect the Whole World", *Wired*, 19 de enero de 2016, disponible en: http://bit.ly/1ncpvOg.

aplicarían según las condiciones específicas de un país como las descriptas en la Parte I.B. Con esa finalidad, recabé información de debates anteriores sobre otros temas clave, a saber, la tipología de las prácticas *zero-rating* y las barreras a la conectividad. Esto debería ampliar el entendimiento de cómo se aplica el análisis de los derechos humanos a estas cuestiones.

III.A. Objetivo legítimo

Los Estados están bajo creciente presión por cerrar la brecha digital global. Los Objetivos de Desarrollo Sostenible de las Naciones Unidas obligan a los Estados a "aumentar de manera significativa el acceso a la información y a la tecnología de la comunicación y a luchar para poder brindar acceso universal y asequible a internet en los países menos desarrollados para el 2020".[340] Si el objetivo de un Estado por cumplir con lo antes detallado es o no legítimo al proponer restricciones sobre la neutralidad de la red, como la fijación de precios diferenciales, dependerá de las condiciones sociales, económicas y políticas del país en cuestión. Los Estados con los niveles de conectividad más altos, ya sea alámbrica o móvil, o ambas, enfrentarán desafíos distintos comparados con aquellos Estados con grandes porcentajes de población que están del lado equivocado de la brecha digital. La mayoría de los Estados en esta última categoría son países en vías de desarrollo, donde vive la vasta mayoría de las personas desconectada0s.[341] Por consiguiente, es más fácil para un país como Zambia, donde menos del 20% de su población tiene acceso a internet, reclamar que al promover el *zero-rating* está fomentando el objetivo legítimo del Estado, es decir, promoviendo la conectividad, que para los Estados Unidos, debido a que su tasa de acceso es de casi 90%.[342] La clave para entender el elemento del objetivo legítimo, sin embargo, no son las tasas de penetración de internet *per se*, sino las barreras a la conectividad que mantienen esas tasas bajas en muchos países.

Para fomentar un objetivo legítimo, las políticas *zero-rating* de los países en vías de desarrollo deben abordar las principales barreras a la conectividad. Una de las barreras primarias es el costo relativamente alto del acceso a los datos vía internet en las plataformas alámbricas y móviles. Una de las razones por la cual el acceso a internet es mucho mayor en los países desarrollados es la asequibilidad relativa. Como regla, dichos países tienen

[340] Naciones Unidas, "Objetivos de Desarrollo Sostenible", 9.c, disponible en: http://bit.ly/1Qk5cqI, último acceso: 31 de julio de 2016.

[341] *Véase*, *supra* notas 133-167 y texto acompañante.

[342] "Freedom on the Net: United States 2014 Scores", *supra* nota 229.

ingresos per cápita mayores y tasas de desigualdad menores que los países en vías de desarrollo. Las tasas de penetración alámbrica y móvil son elevadas, ya que muchas más personas pueden acceder al equipo físico y a los planes de datos necesarios. Existen pocas barreras a la conectividad difíciles para la mayoría. Y hay menos barreras "blandas" como los niveles bajos de educación y de alfabetización que pueden mantener a las personas fuera de internet incluso cuando el acceso es asequible. Para resumir, las barreras a la conectividad no son tan elevadas en los países desarrollados, en caso de que las hubiera, como sí lo son en la mayor parte de los países en vías de desarrollo. Los gobiernos de los países desarrollados generalmente enfrentarán una ardua batalla para justificar las restricciones a la neutralidad de la red y permitir el *zero-rating* como medio para mejorar la conectividad.[343]

Debería ser evidente en estos momentos que generar mayores oportunidades de conexión para los sectores de la sociedad sin derechos digitales puede promover de manera sustancial la concreción de la libertad de expresión y otros derechos humanos básicos en cualquier país marcado por una brecha digital significativa.[344] Los beneficios de aumentar el acceso en los países en vías de desarrollo están muy bien establecidos, por lo cual no vale la pena volver a repetirlos. Por todo lo expuesto, los planes *zero-rating*, si bien son discriminatorios por razones económicas, podrían constituir una "diferenciación legítima" conforme al derecho de los derechos humanos si cumplieran con otros elementos de la prueba del régimen de excepciones.[345] Los Estados en vías de desarrollo con brechas digitales que optan por fomentar este objetivo tendrán probablemente un objetivo legítimo. La expansión del acceso a internet no es menos esencial para alcanzar la libertad de expresión y otros derechos humanos básicos que garantizar el derecho general de impartir o recibir información de manera no discriminatoria, que es lo que logra la neutralidad de la red. Entonces, el principal desafío para

[343] Carta abierta, *supra* nota 111. "En las economías avanzadas como las de la Unión Europea, no existen argumentos para el *zero-rating* como trampolín potencial hacia internet para los usuarios que ingresan por primera vez". Esto no significa que los países desarrollados no podrían justificar las prácticas *zero-rating* apuntando a otros objetivos potencialmente legítimos incluso, quizás, la promoción de las formas no dañinas del *zero-rating* del sector público y privado que fomentan el interés público o el bienestar sin causar un impacto indebido sobre la competencia, la innovación y expresión.

[344] *Véase*, *supra* notas 1333-200 y texto acompañante.

[345] *Véase*, *supra* nota 306 y texto acompañante. ("El principio de la igualdad algunas veces requiere que los Estados parte adopten acciones afirmativas con el fin de disminuir o eliminar las condiciones que causan o ayudan a perpetuar la discriminación prohibida [por el derecho internacional]").

la mayoría de los Estados que luchan por cerrar la brecha digital a nivel local mediante la promoción de una mayor conectividad será si las medidas propuestas son necesarias *y* proporcionales, así como prescriptas por ley.

III.B. Necesidad

La necesidad es una cuestión fáctica. Qué restricciones son indispensables para abordar el problema o desafío reconocido *en un contexto dado* dependerá de: (a) el alcance de su efectividad; (b) la naturaleza del problema a resolver; (c) la existencia de alternativas viables; y (d) la efectividad de esas alternativas. Es importante observar que "necesario" no significa "exclusivo", especialmente cuando los desafíos que se deben enfrentar son considerables o complejos. Un tema relacionado es quién está mejor posicionado para determinar cuándo una medida en particular resulta "necesaria" para cumplir con los objetivos establecidos y cuándo no. A los fines de la presente discusión, las referencias a las "prácticas *zero-rating*" se relacionarán con aquellas descriptas en la tipología presentada en la Parte I.A descripta anteriormente.

Existe evidencia de que las prácticas *zero-rating* pueden incrementar la cantidad de personas que tienen acceso a, por lo menos, partes de internet, y en algunos casos a toda la internet, mediante la reducción de los costos de acceso.[346] "Por ejemplo, en menos de un año, la iniciativa *zero-rating* de Facebook denominada Internet.org ganó más de 9 millones de usuarios [nuevos]".[347] Según Facebook, más de la mitad de esos usuarios pagaron por tener acceso adicional a internet dentro de los 30 días de haberse unido a dicha iniciativa.[348] Con certeza, muchos gobiernos han apostado a que este enfoque se vería en la práctica al promover o condonar las plataformas *zero-rating* como un medio para fomentar la conectividad y, por ende, el desarrollo[349]. Unos pocos críticos del *zero-rating* sostienen que ofrecer un costo reducido o el libre acceso a algunos servicios de internet puede operar en favor del aumento de las suscripciones móviles y de la conectividad. En cambio, la mayoría de los críticos centran su atención en los *daños* percibidos que fueron generados por dichas prácticas –la creación de "jardines vallados" para los

[346] *Véase*, "One Year In", *supra* nota 50.

[347] Estudio de Stanford, *supra* nota 24, en ¶ 5.

[348] *Véase*, "One Year In",*supra* nota 50.

[349] *Véase*, *supra* nota 34 y texto acompañante; *véase además*, por ejemplo, Babu, Anita, "Zuckerberg to Visit India on Oct. 28, First After Internet.org Rebranding", Business Standard, 17 de octubre de 2015, disponible en: http://bit.ly/2fUy9y.r

usuarios o el impacto sobre la competencia– que según sostienen han sobrepasado los beneficios potenciales.[350] A pesar de ello, no hay duda de que se necesita mayor investigación empírica para confirmar las situaciones bajo las cuales las prácticas *zero-rating* pueden ser efectivas con el fin de superar la barrera crucial de los altos costos de acceso, el alcance de esa efectividad y las consecuencias compensatorias de adoptar dichas prácticas.[351]

Lo mismo ocurre con las prácticas *zero-rating* falsas o no selectivas que suponen facilitar la conectividad pública a un costo reducido sin ofender la neutralidad de la red, quizás en mayor grado.[352] A partir de este trabajo, hay muy pocos datos o análisis disponibles sobre el impacto y la efectividad de las *alternativas* para *zero-rating* como tal, si bien hay iniciativas importantes en camino para cambiar esa cuestión. Por ejemplo, Mozilla está investigando los efectos de sus iniciativas de "igualdad de tasa" en este campo.[353] Otro ejemplo es el que brinda la red comunitaria cuyos defensores dicen expande la conectividad total tanto para zonas rurales como urbanas.[354] Estas iniciativas, para responder a las preguntas planteadas por la necesidad que deriva del régimen de excepciones, tendrían que determinar las consecuencias positivas y negativas para la libertad de expresión al implementar una *alternativa* particular con *zero-rating* en un contexto dado, y comparar esos resultados con otros similares obtenidos por las prácticas *zero-rating* llevadas a cabo de la misma forma o en una situación similar. No hay otra forma de saber si las prácticas *zero-rating* logran un nivel de conectividad mayor, similar o menor al que "se podría haber logrado mediante otras formas que no restrinjan la libertad de expresión".[355]

La conclusión es que estamos muy lejos de poder decir con certeza que los enfoques para mejorar la conectividad *zero-rating* son mucho más o menos efectivos para cerrar la brecha digital en un lugar específico que cualquiera de las alternativas comunes. A esto podemos agregar la magnitud de los desafíos sociales, económicos, políticos y culturales que enfrentan los Estados en el mundo en vías de desarrollo, que buscan establecer el acceso a internet para su población,[356] y resulta imposible excluir *ab initio*

[350] *Véase*, Carta abierta, *supra* nota 8.

[351] *Véase*, Thakur, *supra* nota 24.

[352] *Véase*, por ejemplo, "TRAI Consultation Paper", *supra* nota 21, ¶ 18.

[353] *Véase*, Estudio Mozilla, *supra* nota 24.

[354] *Véase*, FGV Direito Rio, "Community Networks: Lesson [sic] from International Practice", YouTube, 29 de abril de 2016, disponible en: http://bit.ly/2geo0NJ.

[355] *Ibíd*., ¶ 33.

[356] *Véase*, *supra* notas 127-166 y texto acompañante.

cualquier enfoque supuestamente viable como innecesario, incluso si ofende a la neutralidad de la red. Asimismo, existe una buena razón para creer que el principal problema abordado –cerrar la brecha digital en aquellos países donde es más predominante– es lo suficientemente considerable y complejo para requerir una respuesta plenamente diversificada.[357] Por esas razones, no es posible a esta altura simplemente descartar las prácticas *zero-rating* como innecesarias o descartables bajo el argumento de que no son lo suficientemente efectivas o que existen mejores alternativas disponibles que pueden lograr los mismos o mejores resultados. Esto significa que el terreno más fértil para las críticas de las prácticas *zero-rating* en estas situaciones es el que ofrece la evaluación de la proporcionalidad.

III.C. Proporcionalidad

En el centro de la proporcionalidad está el equilibrio entre la promoción del objetivo legítimo identificado y el costo de los derechos humanos por lograrlo.[358] Si una restricción propuesta sobre la libertad de expresión promueve un objetivo lo suficientemente efectivo para ser considerado necesario, la pregunta a considerar es si ha sido establecido de forma apropiada para que los beneficios de aprobar ese objetivo superen las consecuencias negativas de manera tal que justifiquen la restricción de ese derecho subyacente. "Al evaluar la proporcionalidad de una restricción sobre libertad de expresión en internet, el impacto de esa restricción sobre la capacidad de internet de proporcionar resultados positivos sobre la libertad de expresión debe ser comparado con los beneficios en términos de protección de otros intereses".[359]

En otras palabras, la proporcionalidad solamente puede ser determinada con referencia a una situación particular y circunstancias específicas. Las excepciones que se propagan tan ampliamente pueden amenazar con "fagocitar la regla",[360] mientras que aquellas que brindan beneficios mínimos o negativos posiblemente no promocionarán un objetivo legítimo. Finalmente, para que esas medidas alcancen el mismo nivel conforme a este estándar legal, deberían ser lo menos intrusivas posible para garantizar los fines deseados.[361] Si no lo

[357] *Véase*, Carrillo, Arturo J., "Comment on Differential Pricing for Data Services (in India)", 30 de diciembre de 2015, en 6 (manuscrito no publicado) (en archivo con autor).

[358] Para un debate más minucioso de la naturaleza y del rol de la proporcionalidad en la adjudicación de los derechos humanos. *Véase*, Legg, *supra* nota 325, cap. 7.

[359] Declaración Conjunta, *supra* nota 10, ¶ 1(b).

[360] *Véase*, *supra* nota 319 y texto acompañante.

[361] *Véase*, *supra* nota 329 y texto acompañante.

fuesen, el equilibrio se inclinaría *contra* la legalidad de dicha medida. En conclusión, una vez que los demás elementos del régimen de las excepciones se alcancen, si la práctica con *zero-rating* propuesta es proporcional o no es una cuestión fáctica del equilibrio relativo entre las ventajas y las desventajas.[362]

Existen varios factores para tener en cuenta al realizar el análisis de equilibrio de la proporcionalidad, punto del debate del *zero-rating* dónde la mayoría o todos los países en vías de desarrollo deberían concentrarse. Los factores generales incluyen el *tipo* de práctica *zero-rating* en cuestión, su *configuración* particular y los *beneficios* percibidos en relación con el objetivo legítimo;[363] *la naturaleza del acceso a internet* y el contenido ofrecido; la existencia y la *efectividad comparable* de las alternativas que no afectan la neutralidad de la red; y otras *consecuencias negativas* de la práctica *zero-rating* sobre el goce de los derechos humanos fundamentales de los usuarios.[364] El Center for Democracy and Technology ha desarrollado un marco adicional de factores más específicos que sirven para mejorar la identificación de "beneficios y daños potenciales" de ciertas prácticas *zero-rating.*[365] Estas prácticas incluyen el principio de la no exclusividad, la presunción contra planes de datos patrocinados, la atención a la seguridad de datos y la privacidad, el suministro de asistencia técnica y la capacitación en los mercados locales, la transparencia y la regulación.[366] La función que cumple este marco puede resumirse de la siguiente manera:

> Con respecto a los proveedores de servicios, la preocupación predominante es el potencial para la distorsión del mercado, ya que como proveedores son excluidos de los acuerdos preferenciales o son obligados a modificar su contenido y servicios para beneficiarse de ellos. Entonces, ya sea que los acuerdos sean exclusivos (especialmente para las compañías afiliadas del operador de red), patrocinados o limitados a fuentes o tipos de contenido y aplicaciones particulares, son todas consideraciones muy relevantes. Para los usuarios, la habilidad de mantener el control del contenido y los servicios a los que ellos acce-

[362] *Véase*, Legg, *supra* nota 325, ¶ 181 (describe la proporcionalidad como prueba legal centrada en "evaluar los efectos colaterales" de la restricción propuesta).

[363] *Véase*, *supra* Parte I.A.

[364] *Véase*, Legg, *supra* nota 325, en ¶181 (La prueba de "proporcionalidad legal [conlleva] la evaluación de los efectos colaterales, medios, e incluso los fines de la acción").

[365] Center for Democracy & Technology, "Zero Rating: A Framework for Assessing Benefits and Harms Executive Summary", 2016, disponible en: http://bit.ly/2gdfwa0.

[366] *Ibíd*., ¶¶ 22-23.

> den o crean a través de internet es la mayor consideración. La elección del usuario por el contenido *zero-rating*, la disponibilidad y el costo del contenido medido y la transparencia de los acuerdos de *zero-rating* son factores significativos para determinar si el *zero-rating* puede estimular la adopción de la banda ancha y el acceso a una internet abierta. Finalmente, si el *zero-rating* servirá como trampolín para el acceso "total" a internet o como rotonda de ofertas conservadas que los usuarios abandonan solo con gran esfuerzo y muchos gastos, dependerá de algunos atributos fundamentales del mercado de la banda ancha: niveles de adopción y despliegue existentes, competencia y alfabetización y educación digital.[367]

Para entender cómo operan dichos factores, debemos examinarlos en contexto. Analicemos el ejemplo de Zambia, descripto en la Parte I.B.III. Una de las primeras críticas a la plataforma Internet.org/Free Basics que opera en Zambia, una práctica compuesta de *zero-rating*, ha sido que ofrece solamente acceso limitado a ciertos sitios y servicios selectos en internet según decisión de Facebook[368] (en asociación con Airtel, la compañía de telecomunicaciones local), creando una internet "para las personas pobres". Las críticas sostienen que, además de violar la neutralidad de la red en principio, este modelo del *zero-rating* compuesto crea un "jardín vallado" ingrato, que es "absolutamente inapropiado" porque "genera una experiencia sintética 'en línea' para los usuarios, que no es realmente la internet".[369] Reclaman, además, que, en los países en vías de desarrollo como Zambia, las plataformas *zero-rating* como Internet.org/Free Basics pueden tener consecuencias económicas discriminatorias al "empoderar la concentración de mercado, restringir la innovación local y reducir sus opciones.[370] Todas estas preocupaciones imperiosas pueden colocarse del lado de las "consecuencias negativas o potencialmente negativas" de la proporcionalidad. Pero deben compararse frente las "consecuencias positivas y potencialmente positivas" del otro lado.

Hay beneficios tangibles para considerar. Según Facebook, un año después del lanzamiento de Internet.org en Zambia, con su énfasis en brindar

[367] *Ibíd*. Resumen ejecutivo.

[368] *Véase*, Honan, *supra* nota 184.

[369] Crawford, *supra* nota 339.

[370] Soares Ramos, Pedro Henrique, "Towards a Developmental Framework for Net Neutrality: The Rise of Sponsored Data Plans in Developing Countries", disponible en: http://bit.ly/1gXJYmV (resumen).

acceso a un gran abanico de sitios de servicios básicos de interés público,[371] el objetivo de una mayor conectividad ha sido promovido sustancialmente, allí y en otros lugares:

> Internet.org les ofrece a los usuarios nuevos de redes móviles un servicio 50% más rápido después de haber lanzado los servicios básicos gratuitos [que antes de haberlos lanzado], y más de la mitad de las personas que se conectan a la red a través de Internet.org pagan por los datos y por acceder a internet dentro de los primeros 30 días. Estos puntos demuestran que Internet.org no es solamente una herramienta exitosa para ayudar a las personas a estar en línea, sino que enseña el valor de internet y contribuye a acelerar el proceso de adoptarla.[372]

Facebook no es el único que dice que las plataformas *zero-rating* como Internet.org pueden tener efectos positivos en cuanto a mayor conectividad,[373] o que no pueden ser tan perjudiciales para la innovación, la competencia y la elección del usuario como sostienen los opositores.[374] Y si bien el acceso se limita a una serie de sitios seleccionados que ofrecen servicios básicos gratuitos, estos servicios han sido direccionados hacia necesidades y contenido local.[375] Puede observarse también que, en respuesta a estas preocupaciones sobre el impacto de Internet.org en la competencia y la innovación local, Facebook hizo cambios a las especificaciones de su plataforma para hacerla no exclusiva y más accesible a los proveedores de servicios y a los diseñadores de aplicaciones, con el fin de "trabajar con la mayor cantidad de operadores móviles y desarrolladores como sea posible para extender los beneficios de la conectividad a distintas comunidades locales en todo el mundo".[376] Esto pretende reducir el daño a la competencia y a la innovación que una plataforma cerrada podría causar.

El equilibrio requerido por la proporcionalidad entre las ventajas y las desventajas puede solamente enfocarse en relación con el problema subyacente abordado y los obstáculos para resolverlo. En el caso de Zambia (y

[371] *Véase*, *supra* nota 184 y texto acompañante.

[372] *Véase*, "One Year In", supra nota 50; *Véase también*, "Facebook's Internet.org App Offers Free internet Access in Zambia", BGR, 18 de agosto de 2014, disponible en: http://bit.ly/2gc3NqY.

[373] *Véase*, *supra* nota 345 y texto acompañante.

[374] Layton y Elalud-Calderwood, *supra* nota 24, en pp. 28-32.

[375] *Véase*, *supra* notas 184 y texto acompañante.

[376] *Véase*, "One Year In", supra nota 50.

otros países en vías de desarrollo), esto significa la brecha digital local y las barreras a la conectividad. A pesar de la mejora en años recientes, Zambia aún clasifica como una de las naciones "menos desarrolladas" en el mundo según las Naciones Unidas.[377] Las tasas de penetración de internet son muy bajas: menos del 2% de la población tiene acceso a internet alámbrica en sus hogares, y es improbable que las rígidas barreras para una mayor conectividad permitan muchas más mejoras en este frente. Por otro lado, la cantidad total de usuarios de internet es aproximadamente del 15%, gracias a una cobertura mucho mayor de telefonía móvil en la población. Incluso, hay una brecha importante entre ese 15% y el 67% que los teléfonos móviles tienen en general, lo que sugiere una oportunidad para acercar la brecha mediante la promoción de una mayor conectividad móvil.[378] Aquí es donde la plataforma *zero-rating* compuesta, Internet.org/Free Basics, ha entrado en el juego.

Según la situación en Zambia, es posible argumentar desde una perspectiva del derecho de los derechos humanos, a la luz de la profunda crisis de conectividad del país, que los beneficios en términos de un mayor acceso que ofrece Internet.org/Free Basics, aunque limitados a servicios selectos, superan las desventajas de la práctica *zero-rating*, haciendo a esta plataforma apropiada y proporcional según las circunstancias. Este argumento se vuelca en la premisa sobre la aceptación de que la plataforma Internet.org/Free Basics aumenta el acceso entre las personas sin derechos digitales en Zambia y los beneficia de muchas maneras significativas, si bien no ofrece internet plena a todos los que se suscriben. Desde esta perspectiva, algo de internet, con la posibilidad de más internet, es mejor que no tener internet, al menos por el momento.[379] Las barreras a la conectividad, tanto rígidas como flexibles, son superadas tanto por la cantidad de usuarios como por el aumento de su experiencia en línea.[380] Los esfuerzos de Facebook por optimizar la apertura de la plataforma han disminuido el impacto negativo de restringir la neutralidad de la red. Y, de manera crucial, un defensor que

[377] *Véase*, *supra* notas 126-130 y texto acompañante (debate el criterio y el listado actual de los Países menos desarrollados según las Naciones Unidas).

[378] *Véase*, *supra* notas 123 y 186 y texto acompañante.

[379] Esto es una opinión común en los países en vías de desarrollo. Véase, Hill, Liezel, y Martínez, Andrés R., "Kenya Says that Access Trumps 'First World' Problem of Net Neutrality", Bloomberg Business, 24 de febrero de 2016, disponible en: http://bloom.bg/1nOJCCc,

[380] El ministro de información, comunicaciones y tecnología de Kenia Joe Mucheru opina que las "personas que no tienen acceso a internet a menudo no comprenden su valor. El acceso a servicios como Free Basics conlleva concientización y, a menudo, están dispuestos a pagar para poder acceder a más herramientas e información".

reclama que Internet.org/Free Basics es una restricción proporcional sobre la neutralidad de la red en Zambia puede argumentar de manera creíble que no existen alternativas mejores o menos intrusivas que la plataforma compuesta *zero-rating*. Si estas premisas sostienen el argumento a favor de los derechos humanos en respaldo de Internet.org/Free Basics en Zambia y otros países en desarrollo de este modo, es indiscutible.

III.D. El *zero-rating* en contexto

Las secciones precedentes subrayan la importancia de evaluar la neutralidad de la red y las excepciones con zero-rating en contexto. La situación en Zambia refleja un polo del espectro de los derechos humanos porque se califica como "país menos desarrollado" con grandes barreras a la conectividad. Por las razones antes debatidas, Zambia seguramente cumpla de manera más efectiva con sus obligaciones de derechos humanos internacionales al permitir las prácticas zero-rating de lo que lo haría si las prohibiera. Del otro lado del espectro, están los países desarrollados como Holanda y los Estados Unidos que prohíben y permiten de manera parcial el zero-rating, respectivamente. En esos países, tanto el acceso a internet en el hogar como móvil es asequible y ubicuo.[381] Las protecciones a la neutralidad de la red son fuertes y las excepciones están muy poco definidas, al menos en el caso de Holanda.[382] En ese país, hay pocas barreras a la conectividad como una cuestión práctica, entonces toda lógica para respaldar la imposición de restricciones sobre la neutralidad de la red debe estar justificada en algún *otro* objetivo reconocido como legítimo, sumado al requisito de que el medio debe ser necesario y proporcional para lograr el objetivo legítimo. Entonces, por ejemplo, las medidas razonables para la administración del tráfico de internet que transgreden la neutralidad de la red se consideran (como en la mayoría de los países) justificadas porque son necesarias, proporcionales y limitadas en el tiempo.[383] Para resumir, Holanda seguramente cumpla de manera más efectiva con sus obligaciones de derechos humanos internacionales al *prohibir* el *zero-rating* en lugar de *permitirlo*.

Todavía no queda claro cómo la Comisión Federal de Comunicaciones interpretará las nuevas normas de los Estados Unidos que permiten los "datos

[381] *Véase*, *supra* notas 228-244 y texto acompañante; véase también, Mayer, David, "Dutch and Slovenian Regulators Nail Carriers Over Net Neutrality", Gigacom, 27 de enero de 2015, disponible en: http://bit.ly/2gKrlqr.

[382] *Ibíd*. *Véase*, Informe Public Knowledge de Rossini y Moore, *supra* nota 24, p. 35.

[383] *Véase*, McCarthy, *supra* nota 21.

patrocinados".[384] ¿Cuándo un plan de datos patrocinados o con *zero-rating* no se basa en una discriminación "injusta" o "no razonable" que viola la neutralidad de la red? Prácticas previas de la Comisión Federal de Comunicaciones respaldan el reclamo realizado por algunos expertos de que las excepciones limitadas a los controles de precios con intereses públicos claros o beneficios para los consumidores podrían sobrevivir el escrutinio caso por caso de la Comisión donde no se percibe impacto negativo o solo un poco en la competencia o en la elección del consumidor.[385] Si sobrevivirían al análisis de los derechos humanos es otro tema.[386]

Existe un punto medio entre los dos polos. Estados como Eslovenia y Chile, que manifiestan características tanto de países desarrollados como en vías de desarrollo, plantean los casos más difíciles.[387] Aquí, el análisis requerido por el derecho internacional de los derechos humanos es más complicado porque los factores a equilibrar tienden a nivelarse. Por ejemplo, Chile goza de niveles relativamente altos de acceso a internet y asequibilidad, lo que lleva a tasas de penetración sustanciales, si bien no tan altas como las de países desarrollados como Holanda, que prohíbe el *zero-rating* de manera categórica.[388] Algunas barreras a la conectividad permanecen, si bien son menores que aquellas en los países en vías de desarrollo. Incluso, los niveles de desigualdad en Chile son elevados, y grandes sectores de la sociedad permanecen desconectados.[389] El sector de las telecomunicaciones está privatizado y es altamente compe-

[384] *Véase*, *supra* nota 240 y texto acompañante. A la fecha, se han presentado demandas o se ha amenazado con hacerlo contra los planes de datos patrocinados por Comcast (Stream TV), Verizon (FreeBee), y T-Mobile (Binge On), entre otros. *Véase*, Lyons, Daniel A., "Usage-Based Pricing, Zero-Rating, and the Future of Broadband Innovation", Boston College Law School Faculty Papers, 4 de enero de 2016, disponible en: http://bit.ly/2eYJKjf (se argumenta que la CFC no debe interpretar las protecciones de neutralidad de la red en términos muy restringidos en relación con prácticas innovadoras de *zero-rating* que benefician la elección del consumidor pero no causan ningún daño a la competencia).

[385] *Véase*, *supra* nota 70 y texto acompañante. Los expertos legales en comunicaciones para los veteranos de los Estados Unidos señalan de forma repetida el hecho de que la Comisión Federal de Comunicaciones permite los números gratuitos como ejemplo de cómo el interés público puede de manera exitosa impulsar excepciones políticas en las normas de fijación de precios de las telecomunicaciones. Los números gratuitos son pagados frecuentemente por las compañías patrocinadoras que permiten a los consumidores comunicarse en forma "gratuita" con las compañías. Véase, "What is a Toll Free Number and How Does it Work?", FCC, 3 de noviembre de 2015, disponible en: http://fcc.us/2fKCTJg.

[386] *Véase*, Carrillo y Nunziato, *supra* nota 233.

[387] *Véase*, *supra* Parte I.B.

[388] *Véase*, *supra* nota 112 y texto acompañante.

[389] *Véase*, *supra* Parte I.B.III.B. (Estudio de caso: país Chile).

titivo, con más opciones para el consumidor. Por ende, es difícil decir si las prácticas *zero-rating*, hasta el punto que son permitidas en Chile, podrían ser justificadas conforme al régimen de derechos humanos sin analizarlas caso por caso a la luz del marco expuesto anteriormente. El punto aquí es no ofrecer una declaración definitiva del cumplimiento de Chile con sus obligaciones de derechos humanos (o de otro país). En su lugar, la idea es ilustrar cómo un marco analítico más riguroso puede aplicarse a dichas cuestiones de política para ampliar su consideración constructiva. Esta "nueva" perspectiva sobre la neutralidad de la red y el *zero-rating* sienta las bases para una investigación normativa y una consideración más profunda de estas cuestiones.

Conclusión: tener el oro y el moro

Resulta que, en ciertas circunstancias, el *zero-rating* puede ser compatible con la neutralidad de la red como norma de derechos humanos. En otras palabras: a veces, uno *puede* tener el oro y el moro. Pero la realidad normativa no responde en sí misma a la pregunta subyacente de *cuándo* se cumplen los requisitos necesarios en un país específico o mediante *qué* acuerdo específico con *zero-rating*, de manera tal de justificar la práctica en este sentido. Para ello, uno debe involucrarse con el marco jurídico de los derechos humanos como se explicó anteriormente. En la Introducción, hice referencia a los debates polémicos sobre la neutralidad de la red en India durante el 2015 para ejemplificar el enigma del *zero-rating* en acción. A pesar de algunos avances, India continúa siendo un caso de estudio ideal de los desafíos que implica la regulación efectiva de la neutralidad de la red.

La pregunta inicial planteada de manera provocativa en la Introducción fue si Facebook en India podía "tener el oro y el moro" al promover su plataforma Internet.org/Free Basics con *zero-rating* y al mismo tiempo proclamarse defensor de la neutralidad. El ente regulador de India decidió en febrero de 2016 que no podía, mediante la prohibición de la fijación de precios diferenciales por parte de las compañías de telecomunicaciones, suspender Internet.org/Free Basics u ofertas similares.[390] De manera sorprendente, sin embargo, el ente regulador de India hizo un "cambio brusco" vergonzoso al emitir dos consultas nuevas relacionadas con la neutralidad de la red,[391] que los defensores creen amenazan con volver a introducir el

[390] *Véase*, *supra* nota 20 y texto acompañante.

[391] Kasuhik, Manu, "TRAI's Web of Confusion", Business Today, 31 de julio de 2016, disponible en: http://bit.ly/2gdkNOR.

zero-rating "por la puerta trasera".[392] Este enfoque "confuso" para regular la neutralidad de la red en general, y el *zero-rating* en particular, confirma que la pregunta sobre qué acuerdos podrían constituir restricciones aceptables sobre la neutralidad de la red en India están por decidirse.[393] También significa que India continúa su lucha contra el enigma del *zero-rating*.

Una mejor manera de reformular la pregunta inicial es si India, al decidir prohibir la fijación de precios diferenciales y el *zero-rating* del sector privado, maximiza el goce de los derechos humanos fundamentales como la libertad de expresión en su población y entonces cumple con las obligaciones de los derechos humanos internacionales. Si consideramos el marco legal internacional descripto en las partes precedentes y la amplia brecha digital de India,[394] la respuesta probablemente sea *no*. Esta "nueva" perspectiva respalda la postura de que, al volver a enmarcar el debate de la neutralidad de la red en términos de derechos humanos, los entes reguladores y los defensores en India y en otros lugares obtendrían un enfoque más consistente y abarcativo para evaluar estas cuestiones. Este, en cambio, fomentaría más debates constructivos y finalmente, mejores políticas. El cambio súbito de opinión en los entes reguladores de India podría ser una señal de una oportunidad para volver a evaluar su postura en aquellos términos.

[392] Singh, Parminder Jeet, "Free Basics, Through the Back Door", The Hindu, 5 de julio de 2016, disponible en: http://bit.ly/29ew1xt.

[393] Kasuhik, *supra* nota 392.

[394] *Véase*, *supra* nota 124 (tabla 2). En India, menos del 20% de la población tiene acceso a internet de algún tipo.

Capítulo Cinco

El "derecho al olvido" de Europa en América Latina

Daphne Keller[1]

Resumen ejecutivo

El presente artículo aborda las tensiones existentes entre el llamado "derecho al olvido" y los derechos a la libertad de expresión e información de los usuarios de internet, en especial, en tanto y en cuanto esos derechos estén reconocidos en América Latina. Se analizarán los sorprendentes acontecimientos ocurridos de acuerdo con dos fuentes jurídicas europeas: el caso "Google Spain"[2] del año 2014 resuelto por el Tribunal de Justicia de la Unión Europea (TJUE), que le exigió al buscador de internet que eliminara determinados resultados de búsqueda; y el Reglamento General de Protección de Datos (RGPD), aún pendiente, de la Unión Europea (UE).

El RGPD es la única reforma efectuada en diez años de la Ley de Protección de Datos de la UE. Entrará en vigor y desplazará a la anterior Ley de Protección

[1] Daphne Keller es Directora del Área de Responsabilidad de los Intermediarios de *Stanford Center for Internet & Society*. Anteriormente se desempeñó como Consejera General de Responsabilidad de los Intermediarios y Libertad de Expresión para Google. En dicho cargo, se concentró principalmente en cuestiones jurídicas y políticas fuera de los EE.UU., incluido el "derecho al olvido", en constante evolución, de la Unión Europea. Como parte de sus funciones anteriores en Google, lideró los equipos legales para Búsquedas Web, Derechos de Autor y Software de Código Abierto. Daphne ha enseñado Derecho de Internet en la Escuela de Derecho de U.C. Berkeley, y también ha enseñado en la Escuela de Información de la misma universidad y en la Escuela de Derecho de Duke. En sus actuaciones en la materia, Daphne ha declarado ante la Investigación Leveson y el Comité Parlamentario sobre Privacidad. Daphne realizó su práctica en el grupo de Litigios de Munger, Tolles & Olson y es graduada de la Facultad de Derecho de Yale y de Brown University. El presente artículo es una versión traducida al español del original en inglés.

[2] Tribunal de Justicia de la Unión Europea, caso C-131/12, "Google Spain SL vs. Agencia Española de Protección de Datos", sentencia del 13 de mayo de 2014, ¶ 94, disponible en: http://bit.ly/2fbElQH.

de Datos en el año 2018. Sus nuevas cláusulas sobre derecho al olvido inclinan el campo de juego fuertemente a favor de eliminar los datos en línea, causando un serio desequilibrio entre los derechos a la expresión y a la intimidad.

Los legisladores y los defensores de América Latina tienen la oportunidad de evitar este desequilibrio en sus propias leyes. En rigor de verdad, existen fuertes argumentos que sostienen que el RGPD podría no satisfacer ciertos requisitos jurídicos y constitucionales e incumplir compromisos de derechos humanos en la región. Los legisladores pueden proteger los derechos a la intimidad y a la protección de datos rechazando cualquier perjuicio a la libertad de expresión, que podrían causar leyes del derecho al olvido mal diseñadas.

El presente artículo: (1) examinará el contexto jurídico del derecho al olvido en Europa y su relación con otros regímenes de "notificación y baja" de la comunicación en internet; (2) analizará las restricciones sustantivas y procedimentales a la libertad de expresión conforme la ley, con un enfoque sobre las nuevas disposiciones del RGPD; y, finalmente, (3) identificará las diferencias principales entre las leyes de la UE y aquellas que rigen en muchos países de América Latina.

Las diferencias entre el sistema legal europeo y el latinoamericano sugieren el siguiente enfoque posible para los formuladores de políticas encargados de elaborar propuestas sobre el derecho al olvido en el ámbito de la legislación, los litigios y la aplicación administrativa:

1. No tratar a los intermediarios como responsables de los datos divulgados por los usuarios, ni definir obligaciones más flexibles para los responsables en relación con la expresión.
2. No imitar el proceso de notificación y baja establecido en el RGPD. Por el contrario, recurrir a la Ley de Responsabilidad de los Intermediarios y a las declaraciones de políticas para identificar cualquier obligación y garantizar el control procedimental contra el exceso de eliminación.
3. Comparar propuestas sobre el derecho al olvido con el marco de derechos humanos de América Latina, que es distintivo y promueve la libertad de expresión.
4. Comparar cualquier propuesta de derecho al olvido con los derechos existentes basados en la intimidad, difamación u otros recursos jurídicos. Identificar si el derecho al olvido respaldaría denuncias que aún no están incluidas en esas leyes, ya sea que las mismas sean deseables en cuestiones de políticas, y determinar las protecciones a la libertad de expresión cuidadosamente diseñadas que podrían aplicarse.

Introducción

Los recientes avances europeos en materia jurídica respecto del llamado "derecho al olvido" no encuadran correctamente con el marco jurídico y de derechos humanos de América Latina. Estos avances pueden resultar especialmente preocupantes para muchos de los países de América Latina cuyas leyes se basan en la Directiva de Protección de Datos de 1995 de la Unión Europea (UE), la ley que se aplicó en el caso "Google Spain".[3] Si bien, dicho caso solamente involucró a los motores de búsqueda, otros casos posteriores de la UE han buscado aplicar el mismo requerimiento a empresas de hosteo en internet, tales como Facebook. Los legisladores de América Latina deberán decidir sobre cuestiones similares de acuerdo con sus propias leyes. Los planteos generales que surgen de estos avances serán relevantes en cada país donde los legisladores luchen por reconciliar los derechos a la intimidad y a la libertad de expresión en el ámbito de las comunicaciones en línea.

Mi análisis sobre esta temática surge de mi actual trabajo en Stanford y de mi experiencia como abogada para Google. En 2014, viajé con el Consejo Asesor de Google sobre el Derecho al Olvido, y tuve la oportunidad de escuchar el análisis tanto de los expertos independientes que integraban dicho Consejo como de los muchos destacados usuarios que declararon en las audiencias públicas.[4] No pretendo ser experta en derecho latinoamericano, pero incluso el análisis más básico sobre jurisprudencia e instrumentos de derechos humanos sugiere que el derecho al olvido tal como ha evolucionado en Europa no encuadra apropiadamente en América Latina. Espero que este análisis resulte útil para los distinguidos defensores de los derechos humanos de la región a medida que se desarrollan los debates nacionales sobre el derecho al olvido.

[3] En 2012, esta lista incluía a Argentina, Uruguay, México, Perú, Costa Rica y Colombia. Leiva, Aldo M., "Data Protection Law in Spain and Latin America: Survey of Legal Approaches", *American Bar Association International Law News*, Vol. 41, No. 4, 2012, disponible en: http://bit.ly/XJ9xyA En 2016, las leyes de unos catorce países de América Latina y del Caribe incorporaron alguna disposición sobre protección de datos. Rich, Cynthia, "Data Privacy Laws in the Western Hemisphere (Latin America, Caribbean and Canada)", *Bloomberg BNA - World Data Protection Report*, Vol. 16, Nº 6, junio 2016, disponible en: http://bit.ly/2fjXULC; There are economic and other reasons to emulate EU law, as the simplest means to be deemed "adequate" for data transfers to national companies doing business in the EU. Cerda Silva, Alberto, "Personal Data Protection and Online Services in Latin America", disponible en: http://bit.ly/2fjY7y9.

[4] Consejo Asesor de Google sobre Derecho al Olvido, informe final, febrero de 2015, disponible en: http://bit.ly/1r2Vv7e.

I. Análisis

I.A. Orígenes jurídicos del "derecho al olvido" en internet

El llamado "derecho al olvido" recorre una larga historia en el derecho europeo, por ejemplo, en las leyes alemanas formuladas para ayudar a los delincuentes rehabilitados.

Lo inédito del fallo de "Google Spain"[5] fue que el derecho al olvido se basó fuertemente en la amplia y sólida Directiva de Protección de Datos[6]. El derecho articulado en ese caso (obligar a los buscadores a borrar determinados resultados en ciertas búsquedas) no es más que el "derecho a eliminar datos",[7] según muchos afirman. No obliga a borrar páginas web o material de archivos y, ciertamente, no puede controlar la memoria humana. De acuerdo con este razonamiento, la sigla RTBF[8] que nombra al "derecho al olvido" en inglés, sería un nombre inapropiado. De todos modos, la terminología sobre derecho al olvido ha resonado y se ha repetido una y otra vez en todo el mundo, la cual toma vida propia más allá del contexto jurídico de la Unión Europea.

En América Latina, los nuevos casos y las propuestas legislativas sobre derecho al olvido han avanzado rápidamente después de "Google Spain". En algunos casos, las leyes nacionales reconocen los derechos de eliminar cierta información sobre el pasado de una persona, por ejemplo, en cuestiones financieras o penales.[9] En 2015, la Corte Suprema de Colombia emitió un fallo, en el marco del derecho al olvido, que responsabilizó a un editor web y no a los buscadores, justificado en parte por el derecho mediático y

[5] Tribunal de Justicia de la Unión Europea, *supra* nota 2, párr. 94.

[6] Texto de la Directiva de Protección de Datos, disponible en: http://bit.ly/1f9oJZ7.

[7] Tribunal de Justicia de la Unión Europea, *supra* nota 2, párr. 82.

[8] "Right to be forgotten".

[9] Derechos Digitales, "What are the Implications of the Right to be Forgotten in the Americas?", en: *iFex*, 22 de septiembre, 2015, disponible en: http://bit.ly/2eL0DNh; *Véase* Cerda Silva, *supra* nota 3 ("For the Supreme Courts of Argentina and Costa Rica, processing personal data on paid debts infringes fundamental rights, whereas for the Supreme Court of El Salvador it does not.")

el derecho penal.[10] Además, las constituciones de muchos países contienen disposiciones de *habeas data*, que, de acuerdo con algunas opiniones, respaldan derechos similares al derecho al olvido de la Unión Europea.

Los planteos sobre la influencia de la ley de la Unión Europea son especialmente importantes para muchos países de América Latina, incluidos Chile, Argentina, Uruguay, México, Costa Rica, Perú, Nicaragua y Colombia, que poseen leyes directamente modeladas a partir de las leyes de protección de datos de la UE, y para países como Brasil, donde se han propuesto leyes similares.[11] Las legislaturas tienen la gran motivación económica de seguir la ley de la UE a fin de "adecuarse" a la transferencia comercial, o de otra índole, de datos desde dicha región[12]. Por lo general, las disposiciones de protección de datos de América Latina incluyen cláusulas muy similares a aquellas interpretadas en el caso "Google Spain", otorgando a los dueños de los datos el derecho de acceder, de rectificar, de cancelar y de objetar el tratamiento de sus datos personales.[13] Este tipo de procedimientos fueron aplicados por la Agencia de Protección de Datos de México, en el 2015, en una orden vinculada al derecho al olvido posteriormente revertida por el tribunal.[14]

Al mismo tiempo, algunos aspectos del derecho y de la cultura de América Latina difieren ampliamente del derecho al olvido de la Unión Europea. Eduardo Bertoni, actual director de la Agencia de Protección de Datos de Argentina, declaró que el nombre "derecho al olvido" era un "agravio" y escribió que si

[10] Derechos Digitales, *supra* nota 9; Corte Constitucional de Colombia, Sentencia T-277/15, 12 de mayo de 2015, disponible en: http://bit.ly/1iQCR1b; *véase* también Corte Constitucional de Colombia, *"En nombre de un menor vs. Periódico 'El nuevo día' y el Instituto Colombiano de Bienestar Familiar"*, Sentencia T-453/13, 15 de Julio de 2013, disponible en: http://bit.ly/2eAkRJ1 (se trata de un periódico, y no de un buscador, responsable de revelar la identidad de un menor presuntamente víctima de abuso); Corte Constitucional, *"Martínez vs. Google Colombia & Editorial El Tiempo"*, Sentencia T-040/13, 28 de enero de 2013, disponible en: http://bit.ly/1FylMlk (buscador no responsable de acceder, corregir o borrar los resultados de búsqueda sobre un proceso penal del demandante).

[11] Voss, W. Gregory y Castets-Renard, Céline, "Proposal for an International Taxonomy on the Various forms of the 'Right to be Forgotten': a Study on the Convergence of Norms", en: *Colorado Technology Law Journal*, Vol 14, Nº 2, Colorado, Universidad de Colorado, 2016, p. 314

[12] Cerda Silva, *supra* nota 3. Las definiciones de adecuación realizadas por la Comisión Europea conforme la Directiva de 1995 permanecerán en vigor, pero podrían cuestionarse o revocarse en el futuro según el RGPD. *Véase* "The EU General Data Protection Regulation", Hunton & Williams Blog, disponible en: http://bit.ly/2gGDpKi.

[13] Voss y Castets-Renard, *supra* nota 11.

[14] *Ver* nota en: http://bit.ly/2bCBdgg. "Google recurre el primer caso sobre derecho al olvido en México", Derecho al olvido, España, 4 de junio de 2015, disponible en: http://bit.ly/2fBw8dp.

quienes estuvieron involucrados en violaciones de derechos humanos pudieran solicitar a Google que dicha información no fuera posible de encontrar sería "un gran insulto a nuestra historia (por decirlo suavemente)".[15] Como dijo un experto en protección de datos: "No podemos comprender el derecho al olvido como ha sido entendido por el Tribunal de Justicia

Europeo debido a las diferencias culturales".[16] Estas diferencias han sido evidentes en algunos casos anteriores a Google Spain. Por ejemplo, en 2013, la Corte Constitucional de Colombia rechazó dos veces los reclamos vinculados al derecho al olvido contra Google.[17]

La región cuenta con jurisprudencia y legislación sustanciales que protegen el derecho a la libertad de expresión de los usuarios en internet de un modo diferencial respecto de la UE. La aplicación de esos derechos ha sido inconsistente y, en demasiados casos, ha sido víctima de la corrupción política, aunque el marco intelectual y jurídico sigue siendo robusto.[18] El Marco Civil de Brasil establece que las plataformas, en la mayoría de los casos, solo deben retirar el contenido generado por los usuarios si un tribunal lo considera ilícito, y declara que dicha norma es necesaria "para asegurar la libertad de expresión y prevenir la censura".[19] La Ley de Propiedad Intelectual de Chile exige el retiro de información únicamente conforme a una orden judicial.[20] La Corte Suprema de Argentina llegó a una conclusión similar de acuerdo con los primeros principios y derechos constitucionales. En el caso emblemático de Belén Rodríguez, se rechazó la responsabilidad estricta y en su lugar se dictaminó la responsabilidad del intermediario por el conocimiento real del contenido ilícito. El dictamen estableció que las

[15] Bertoni, Eduardo, "El derecho al olvido: un insulto a la historia latinoamericana" *("The Right to Be Forgotten: an Insult to Latin American History"), The Huffington Post*, 24 de septiembre de 2014, disponible en: http://huff.to/1ucd9pk.

[16] Carson, Angelique, "The Responsibility of Operationalizing the Right To Be Forgotten", The International Association of Privacy Professionals (IAPP), 12 de marzo de 2015, disponible en: http://bit.ly/2ek4eRB, citando a la abogada mexicana, Rosa María Franco Velázquez: "En franco contraste, el jefe de la Agencia Española de Protección de Datos declaró que el derecho al olvido 'no afecta el derecho a saber'".

[17] Corte Constitucional de Colombia, *supra* nota 10.

[18] Algunos expertos, incluso, han observado reincidencias en los fallos recientes de la Corte Interamericana. *Véase* http://bit.ly/2gcyV9q.

[19] Ley Federal No. 12.965 del 23/4/2014, disponible en idioma inglés en: http://bit.ly/1gubZiQ.

[20] Ley No. 20.435 del 4/5/2010, Art. 85, disponible en: http://bcn.cl/nol. La Corte Suprema de Chile también respaldó un fallo de apelación que limitaba las obligaciones de las plataformas de internet a eliminar contenido supuestamente difamatorio, también por motivos de libertad de expresión. Corte Suprema, *"Suazo vs. Reclamos.cl"*, 6/07/09, disponible en: http://bit.ly/2f2LoQT.

plataformas deben retirar los datos de internet solo después de la resolución emitida por una autoridad pública competente.[21]

El requerimiento de una orden judicial para retirar contenido de internet marca un contraste con la jurisprudencia europea. En la mayoría de los países, el aviso por parte de los individuos interesados siempre ha sido suficiente para eliminar contenido de internet, sin necesidad de contar con ningún control judicial. La excepción parcial es España. La legislación española inicialmente requería órdenes judiciales, pero la Corte Suprema de España eliminó dicha norma por inconsistente con la Directiva sobre el comercio electrónico de la UE.[22] Posteriormente, un tribunal inferior sostuvo que las consideraciones sobre libertad de expresión de todos modos requerían una orden judicial, excepto en el caso de violaciones a la ley, que resulten "incuestionables, manifiestas y sin lugar a dudas".[23]

La especial preocupación de América Latina respecto de los derechos a la libertad de expresión surge de los instrumentos de derechos humanos que posee la región. El artículo 13.3 de la Convención Americana sobre Derechos Humanos prevé cuestiones relacionadas con la responsabilidad de los intermediarios en la actualidad, al sostener:

> No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.[24]

---

[21] Corte Suprema de Justicia de la Nación argentina, *"Rodríguez M. Belén c/Google y otro s/ daños y perjuicios"*, sentencia R.522, XLIX, 20/10/14, disponible en: http://bit.ly/2f2LoQT. La Corte Suprema de la India arribó a un resultado comparable en "Shreya Singhal vs. Unión de la India", Nº. 167/2012, sentencia del 24 de marzo de 2015.

[22] Tribunal Supremo de Madrid, Sala en lo Civil, *"Asociación de Internautas"*, sentencia Nº 773/2009, del 10/11/09. Disponible en: http://bit.ly/2f76g8H, analizado en: http://bit.ly/2fscOQA.

[23] Tribunal de Apelaciones de Barcelona, *"Royo v Google"*, sentencia 76/2013, 13/02/13; Una serie de casos del Reino Unido también abordó la misma cuestión, pero conforme a la Ley de Difamación Doméstica en lugar de las normas sobre Responsabilidad de los Intermediarios de Comercio Electrónico. De todos modos, el caso *"Davison vs. Habeeb"* (2011) –EWHC 3031 (QB)– sostuvo que la simple acusación de que la publicación de un usuario fuese difamatoria no establecía la obligación de conocimiento o eliminación para el hosteo de un *blog*.

[24] Convención Americana de Derechos Humanos, "Pacto de San José, Costa Rica", disponible en: http://bit.ly/1Ac82L9.

Esta preocupación por la censura indirecta y los controles particulares encuadra perfectamente con leyes que, como en Google Spain, asignan a empresas privadas la adjudicación de derecho al olvido. Lo mismo puede decirse de la garantía del artículo 8 de "un tribunal competente, independiente e imparcial previamente establecido por la ley", y el debido proceso de la prueba de tres partes de la Corte Interamericana para la restricción de contenido.[25]

La Declaración de Principios sobre Libertad de Expresión de la Organización de Estados Americanos también es relevante. La misma establece:

> Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar garantizada solo a través de sanciones civiles, en los casos en que la persona ofendida sea un funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. Además, en estos casos, debe probarse que en la difusión de las noticias el comunicador tuvo intención de infligir daño o pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas.[26]

Este marco de limitaciones a la expresión en relación con la privacidad será de importancia en tanto y en cuanto los firmantes de la Convención deban enfrentar asuntos jurídicos sobre el derecho al olvido.[27]

I.B. Reseña sobre la ley de protección de datos

El derecho establecido en la Directiva de 1995 de la Unión Europea relativa a la protección de los datos, y en muchas leyes latinoamericanas, se distingue de los derechos a la intimidad preexistentes. El derecho a limitar el tratamiento de toda la información relacionada con las personas físicas, y no únicamente la información que infrinja un daño o invada la intimidad personal, es muy abarcativo. La Directiva de la UE establece un marco

[25] *Véase* http://bit.ly/2gD6F4J.

[26] Principio 10, disponible en: http://bit.ly/15lje4M. En algunos sistemas jurídicos, los tribunales pueden aplicarlo como una norma específica para medios de noticias.

[27] Dado que los derechos a la intimidad son anteriores a los derechos a la protección de datos, en la mayoría de los instrumentos jurídicos existen cuestiones importantes respecto de si las antiguas discusiones sobre privacidad aplican a ambos derechos. En este caso, la respuesta pareciera ser afirmativa.

jurídico y administrativo detallado sobre la protección de este derecho, incluidas las bases jurídicas específicas para que los organismos reglamentados efectúen el tratamiento de los datos personales de los individuos. Donde no se cumplan dichas bases, el tratamiento se considerará ilícito.

Los organismos responsables del tratamiento de los datos personales se clasifican generalmente en "controladores" y "procesadores". Los primeros son organismos que tienen datos personales en su poder y deciden qué hacer con los mismos. Dado que son quienes toman las decisiones, asumen más obligaciones conforme la ley que, potencialmente, podrían incluir el cumplimiento con los requerimientos de eliminación de datos o del "derecho al olvido". Los organismos "procesadores" también controlan los datos personales, pero siguen las instrucciones de un organismo "controlador" sobre qué hacer con los mismos. Además, asumen menos deberes jurídicos. En un simple ejemplo, una firma que posee registros sobre sus empleados es un controlador de sus datos personales. Si llegara a tercerizar las operaciones relacionadas con la nómina de pagos mediante un contrato con una empresa responsable de la liquidación de sueldos, dicha empresa sería un "procesador". La decisión del TJUE respecto de que Google actuó como "controlador" de la información indexada en su buscador fue un aspecto clave del caso "Google Spain".[28]

El fallo del TJUE inició el debate crítico respecto de la situación de otros proveedores de servicios importantes, incluidas las plataformas como Twitter o YouTube. Si dichos intermediarios también son controladores, entonces el alcance de la potencial supresión del discurso en internet de acuerdo con el "derecho al olvido" es significativamente más amplio. Existen fuertes argumentos en contra de dicho resultado, por ejemplo, que las plataformas no pueden ser controladores dado que solamente se dedican al tratamiento del contenido siguiendo las instrucciones de un usuario, cuya función es la de controlador. Los pocos casos registrados hasta la fecha han llegado a resultados inconsistentes sobre este asunto.[29] Los argumentos basados en la libertad de expresión contra las obligaciones sobre el "derecho al olvido" para las plataformas son, potencialmente, más fuertes que para los buscadores, dado que retirar información de un servicio de hosteo podría eliminarla

[28] Tribunal de Justicia de la Unión Europea, *supra* nota 2, ¶ 82, p. 85-88.

[29] Compárese, Tribunal Supremo del Reino Unido, "CG vs. Facebook Ireland Ltd. & Anor", sentencia del 20 de febrero de 2015, NIQB 11, disponible en: http://bit.ly/1f9oJZ7 (Facebook es "controlador"), y el caso del blogger español, Sección Primera de la Sala en lo Contencioso-Administrativo de la Audiencia Nacional, Madrid, 2015, disponible en: http://bit.ly/2fezYoK (la plataforma de hosteo de blogs no es un organismo "controlador"; revisión sobre otras bases).

por completo de internet, incluso a veces sin dejar al autor una copia de su trabajo, como ocurrió con la cuenta de un blogger en 2016.[30]

I.C. Ley de Responsabilidad de los Intermediarios

La Ley de Responsabilidad de los Intermediarios limita y define la responsabilidad jurídica de los intermediarios técnicos por el contenido publicado en línea por parte de terceros.[31] La responsabilidad de los intermediarios en la UE se rige según los artículos 12 y 15 de la Directiva sobre el comercio electrónico,[32] conforme su implementación en la legislación nacional de los estados miembros. Los intermediarios protegidos por dicha ley abarcan desde proveedores de acceso a internet, tales como Telefónica, hasta plataformas de redes sociales como Twitter e indexadores de búsqueda como Google, entre otros.

De acuerdo con la mayoría de las leyes de responsabilidad de los intermediarios, las plataformas no están obligadas a supervisar la información publicada por los usuarios y tampoco tienen responsabilidad alguna por el contenido ilícito que desconozcan y que sea publicado por los usuarios. En algunos sistemas jurídicos, incluso el conocimiento de expresiones ofensivas de los usuarios, incluidas las expresiones consideradas como ilícitas por un tribunal, no implica responsabilidad jurídica alguna para los intermediarios. El artículo 230 de la Ley de Decencia en las Telecomunicaciones de Estados Unidos opera de este mismo modo y facilita el increíble auge económico y tecnológico de las empresas de tecnología estadounidenses de las últimas dos décadas, así evita la supresión de expresiones lícitas por parte de intermediarios precavidos que han buscado evitar riesgos. En muchos otros países, existe la obligación de eliminar información, pero se limita a proteger los derechos de los usuarios de internet.

Muchas leyes, incluida la Directiva sobre Comercio Electrónico de la UE, consideran el "conocimiento" como disparador de la acción de los interme-

[30] En 2016, un artista informó que Google había borrado su trabajo de catorce años, incluidas las únicas copias de algunas de sus obras, al haber dado de baja contenido que había publicado en el servicio Blogger de la empresa. Véase "Google's deleted an artist's blog, along with 14 years of his work", Science alert, 18 de julio de 2016, disponible en: http://bit.ly/2aw3Hfw.

[31] Anteriormente, se analizan las leyes latinoamericanas. En Estados Unidos, las leyes principales sobre responsabilidad de los intermediarios son la DMCA 17 USC 512, disponible en: http://bit.ly/24wrfDr; y la CDA 230 47 USC 230, disponible en: http://bit.ly/1hlnlbP.

[32] Parlamento Europeo y Consejo de la Unión Europea, Directiva 2000/31/EC, 8 de junio de 2000, disponible en: http://bit.ly/1xa4aFc.

diarios: una vez que el intermediario es consciente del contenido ilícito, debe darlo de baja o asumir su responsabilidad. Por lo general, las plataformas de comunicaciones operan con sistemas de notificación y baja que eliminan el contenido de los usuarios conforme dichas leyes. En principio, los intermediarios solo deberían remover el contenido de los usuarios si la acusación jurídica de la notificación es correcta y el contenido es realmente ilegal. Sin embargo, en la práctica, los procesos de notificación y baja se utilizan incorrectamente y terminan afectando contenido lícito. Varios estudios confirman que los intermediarios a menudo aceptan pedidos para eliminar información, incluidos los incorrectos.[33] Algunas empresas dedican mucho esfuerzo y recursos para identificar y rechazar solicitudes de eliminación infundadas. Tengo el orgullo de decir que formé parte de dicho esfuerzo en Google. Pero tanto la evidencia anecdótica como estadística indica que dichos esfuerzos, por sí solos, no son suficientes. La eliminación de datos incorrectos de acuerdo con los sistemas de notificación y baja incluye desde contenido religioso,[34] político[35] y científico[36] hasta reseñas de consumidores.[37]

Las cifras detrás de esta problemática son significativas. Los intermediarios reciben *muchos* pedidos falsos de eliminación de datos[38]. En el contexto del "derecho al olvido", Google revela que le han pedido eliminar 1,6 millones de páginas web, y que alrededor del 57% de dichas solicitudes no argumentan un reclamo jurídico válido conforme la extensa Ley del Derecho al Olvido de la UE[39]. El buscador Bing de Microsoft también declara que más de la mitad de los pedidos que recibe relacionados con el derecho

[33] *Véase* la lista disponible en: http://stanford.io/2fBMNhk.

[34] Galperin, Eva, "Massive Takedown of Anti-Scientology Videos on YouTube", Electronic Ford Foundation, 5 de septiembre de 2008, disponible en: http://bit.ly/2eRFGzP.

[35] Rodriguez, Salvador, "Russia, Turkey Asked Twitter To Remove Hundreds Of Tweets As Government Censorship Attempts Skyrocket", International Business Times, 2 de septiembre de 2015, disponible en: http://bit.ly/2fsi7zP.

[36] Timmer, John, "Site plagiarizes blog posts, then files DMCA takedown on originals", Ars Technica, 5 de febrero de 2013, disponible en: http://bit.ly/2ekn5Ms.

[37] Lee, Timothy B., "Criticism and takedown: how review sites can defend free speech", Ars Technica, 1 de junio de 2011, disponible en: http://bit.ly/2dZl1tg.

[38] Véase Urban, Jennifer and Laura Quilter, Laura, "Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act", Santa Clara Computer and Hight Technology Law Journal, Vol. 22, Nº 4, California, Santa Clara University School of Law, 2006; Urban, Jennifer, Karaganis, Joe and Schofield, Brianna L., "Notice and Takedown in Everyday Practice", UC Berkeley Public Law Research, Paper Nº 2755628, 2016, disponible en: http://bit.ly/2ex6YbT.

[39] Google, "European privacy requests for search removals", disponible en: http://bit.ly/1FdZMGD.

al olvido son injustificado[40]. Los organismos reguladores de asuntos de privacidad parecen estar de acuerdo. Una revisión de casos presentada ante las autoridades nacionales concluyó que "en la gran mayoría de los casos, la negativa de un buscador a acceder a un pedido se encuentra justificada".[41]

A fin de contrarrestar el problema de eliminaciones excesivas, los legisladores y defensores de los derechos humanos de todo el mundo han desarrollado normas de procedimientos para notificaciones y bajas. Dichas normas, que incluyen penalidades por notificaciones de mala fe y oportunidades para que las partes acusadas se "contranotifiquen", se proponen controlar la eliminación excesiva de datos. Los Principios de Manila, el "estándar de oro" ampliamente avalado sobre responsabilidad de los intermediarios, enumeran varias herramientas procedimentales, incluidas formalidades de notificaciones y requerimientos de transparencia.[42] Este artículo explorará las protecciones procedimentales para la comunicación en internet en el contexto del derecho al olvido en la sección II.B.

I.D. Conflicto de cuestiones sobre protección de datos y responsabilidad de los intermediarios en el marco del derecho al olvido

Históricamente, pocos abogados han establecido una asociación entre la protección de datos y la Ley de Responsabilidad de los Intermediarios. En la práctica europea, ambos campos utilizan un lenguaje muy distinto, y varios expertos se dedican a su interpretación, aplicación y manejo de litigios al respecto.

El fallo sobre "derecho al olvido" del TJUE en el caso "Google Spain" del año 2014 marcó un cambio. El tribunal determinó que Google actuó como controlador de información en sus resultados de búsqueda, al asumir las correspondientes obligaciones de limitar el tratamiento de los datos ante los pedidos al respecto. La reparación ordenada por el tribunal no fue la eliminación completa de los datos, ya sea de los resultados de la búsqueda o de la infraestructura subyacente de indexación de Google. En su lugar, el buscador fue llamado a quitar los datos de los resultados de búsqueda únicamente cuando los usuarios buscaran el nombre del demandante.[43] El tribunal determinó lo que

[40] Microsoft, "Content Removal Requests Report", disponible en: http://bit.ly/2faRmwc.

[41] Comisión Europea, comunicado de prensa emitido por el Grupo de Trabajo de Protección de Datos del artículo 29, Bruselas, 18 de junio de 2015, disponible en: http://bit.ly/1OoWVnP.

[42] Principios de Manila sobre Responsabilidad de los Intermediarios, http://bit.ly/29PAhDF.

[43] Tribunal de Justicia de la Unión Europea, *supra* nota 2, ¶ 94.

efectivamente es un sistema de notificación y bajas para eliminar resultados de búsqueda, pero arribó a esta reparación mediante el lenguaje y la lógica de la protección de datos, sin hacer referencia alguna a las normas de responsabilidad de los intermediarios de Europa. Los casos posteriores a "Google Spain" probablemente obliguen a los tribunales inferiores a abordar de modo más directo las cuestiones sobre cómo se combinan ambos campos del derecho.

Sin embargo, el marco completo de la Ley de Protección de Datos que subyace el caso "Google Spain" será reemplazado por el RGPD. Por primera vez, la ley establecerá los pasos concretos para la eliminación de datos personales, incluido el contexto del derecho al olvido. También autoriza la aplicación de multas extremadamente elevadas (4% de la facturación global anual o 20 millones de euros) a los controladores que la incumplan.[44] Esta exposición financiera, junto con las disposiciones legales que son ambiguas en el mejor de los casos, o que favorecen fuertemente la eliminación de los datos en el peor de los casos, convierte al RGPD en una mayor amenaza para la comunicación en internet que el marco legal actual de la UE para "Google Spain".

El desfasaje entre los sistemas de notificación y bajas y la Ley de Protección de Datos surge en gran parte al combinar datos de usuarios almacenados de forma privada con información y comunicación disponible para el público. La Ley de Protección de Datos ha sido creada y ha evolucionado como sistema de tratamiento de datos de *back-end* (procesamiento subyacente), es decir, el tratamiento que el banco, el médico o un club podrían hacer de los datos personales, por ejemplo, almacenarlos en sus archivos. Para los intermediarios, el procesamiento *back-end* incluye acciones como rastrear el comportamiento de los usuarios en internet en sistemas de almacenamiento tales como inicio de sesiones, perfiles, o cuentas. La Ley de Protección de Datos aplica a este tipo de datos, y proporciona a los individuos derechos de acceso y eliminación de datos, independientemente de si la empresa es una plataforma intermediaria para contenido generado por los usuarios. El análisis basado en los derechos humanos acerca de las solicitudes de eliminación de datos *back-end* es relativamente directo. Solo dos grupos de derechos están implicados: aquellos pertenecientes al sujeto que solicita los datos, y aquellos de la empresa.

Presuntamente, los derechos de protección de datos del solicitante prevalecerán en la mayoría de los casos. Las normas sobre protección de datos conforme la Directiva de 1995 y el RGPD son ampliamente razonables para esta situación bipartita. Sin embargo, debido al enfoque histórico de la ley respecto de este escenario, el marco jurídico de la protección de datos posee pocas reglas y un

[44] Art. 83 del RGPD.

acotado precedente en el abordaje de la expresión pública a través de internet, es decir, los distintos datos en cuestión en el marco del derecho al olvido.[45]

La solicitud a los intermediarios de eliminar la comunicación en internet de una persona reviste otro carácter desde una perspectiva de derechos humanos. Afecta al menos a cuatro partes: al sujeto que solicita los datos, al intermediario, a la persona que publica el contenido en línea, y a otros usuarios que desean ver el contenido. Los procedimientos diseñados para la eliminación de datos *back-end* y la interacción de dos partes no son suficientes para proteger y equilibrar los derechos de estos cuatro actores tan diferentes. Cuando se aplican a la comunicación en internet, los derechos a la libertad de expresión se ven afectados.

II. Libertad de expresión desde la perspectiva del derecho al olvido

Las preocupaciones de los abogados de derechos humanos acerca del derecho al olvido y la libertad de expresión pueden clasificarse en dos categorías. La primera aborda el derecho sustantivo: ¿deberían las personas poder suprimir información verídica sobre su pasado? De ser así, ¿qué límites deberían establecerse sobre el derecho? La segunda es de carácter procedimental: si existe el derecho al olvido, ¿quién debería encargarse de su aplicación y bajo qué reglas? En el fallo de "Google Spain" y el RGPD, los legisladores de la UE arribaron a respuestas controvertidas a ambas preguntas; respuestas que se encuentran en fuerte tensión con el marco de protección jurídica de América Latina.

II.A. Libertad de expresión y alcance real del derecho al olvido

Como ha dicho Eduardo Bertoni, el derecho al olvido es como el test de Rorschach. Las personas le asignan varios significados. Muchos de ellos involucran daños ya abordados en las leyes existentes que rigen la difamación y otros perjuicios relativos a la reputación y dignidad. Según Joris van Hoboken, dichas leyes "representan doctrinas intricadas para equilibrar los intereses en la sociedad respecto de la publicidad de y/o sobre otros y los in-

[45] Una excepción es la Opinión 1/2008 sobre asuntos de Protección de Datos relacionados con buscadores, WP 148, adoptada el 4 de abril de 2008 (distinción entre "datos de usuario en interfaz *back-end*" y "datos de contenido" indexado), p. 14, disponible en: http://bit.ly/2eo8Ohx.

tereses de privacidad y dignidad de las personas físicas".[46] Sin embargo, para el derecho al olvido, dichas limitaciones, defensas y doctrinas elaboradas aún no existen. Tanto los legisladores como Google deberán reinventarlas.

El tribunal expedido en el caso "Google Spain" declaró que Google debía eliminar los datos inexactos[47] o "inadecuados, no pertinentes y ya no pertinentes, o excesivos en relación con los fines del tratamiento".[48] Esto incluye información verídica[49] e información que no cause perjuicio alguno a la persona que procura su eliminación.[50] El tribunal identificó una excepción:

> Si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate.[51]

El tribunal no se explayó sobre esta prueba de equilibrio de intereses públicos. Sin embargo, advirtió que "como regla", el interés público por la información no prevalece sobre los derechos de las personas a eliminar sus datos.[52] En una omisión sorprendente para muchos defensores de los derechos humanos, el Tribunal no identificó ni analizó los otros derechos a la libertad de expresión que pueden verse afectados: los derechos del webmaster o del editor.[53] El fallo fue objeto de muchas críticas tanto por establecer un estándar impreciso como por priorizar los derechos de protección de datos por sobre los derechos de acceso a la información, en lugar de sopesarlos en términos iguales. De acuerdo con el ex relator especial de Naciones Unidas para la Libertad de Expresión, Frank La Rue, abogado guatemalteco especializado en derechos humanos:

> El derecho a la privacidad y a la protección de datos es un derecho

[46] Van Hoboken, Joris, "The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Freedom of Expression Safeguards in a Converging Information Environment", informe para la Comisión Europea, Amsterdam, mayo de 2013, ¶ 23. Disponible en: http://bit.ly/LrCKYE.

[47] Tribunal de Justicia de la Unión Europea, *supra* nota 2,¶ 92.

[48] *Ibíd*. ¶ 94 (paráfrasis del artículo 6.1(c) de la Directiva).

[49] *Ibíd*. ¶ 92.

[50] *Ibíd*. ¶ 96.

[51] *Ibíd*. ¶ 97.

[52] *Íd*.

[53] Peguera, Miquel, "The Shaky Ground of the Right to be Delisted", en: Journal of Entertainment & Technology Law, Vol. 18, Nº 3, 2016, p. 555, disponible en: http://bit.ly/2ghbOMB (próximamente en 2016) (citas omitidas).

> fundamental íntimamente vinculado al ejercicio del derecho a la libertad de expresión, y deben entenderse como complementarios y nunca en conflicto entre sí. El derecho al olvido como tal, no existe (…). La decisión por parte de una autoridad de eliminar información o bloquear motores de búsqueda solo se puede basar en el hecho de que la forma de obtener dicha información o el contenido de la misma sea maliciosa, falsa, o produzca un serio daño a un individuo.[54]

El planteo de La Rue se basa en los importantes límites reales de la ley antes de Google Spain y de la Convención Interamericana que protegen la comunicación que no es maliciosa, falsa y perjudicial. Este abordaje marca un fuerte contraste con la amplia norma del TJUE, que permite la eliminación de información verídica y no perjudicial. La Rue además ha vinculado la Ley del Derecho al Olvido con cuestiones de violencia política y abusos a los derechos humanos.

En el caso de los derechos humanos, uno de los principios fundamentales para erradicar la impunidad es establecer la verdad de las violaciones a los derechos humanos cuando ocurran. Esto se conoce como el derecho de las víctimas y sus familias a la verdad, pero también de la sociedad en su totalidad para reconstruir la memoria histórica y recordar a las víctimas del pasado.

A pesar de las preocupaciones planteadas por La Rue y otros, las nuevas disposiciones del derecho al olvido conforme al RGPD hacen poco por mejorar sobre la base de la orientación del TJUE. La ley excusa a los controladores de eliminar la información necesaria "para ejercer el derecho a la libertad de expresión e información"[55]. Pero delega en las leyes de los estados miembros de la UE la responsabilidad de definir qué significan verdaderamente esos derechos y cómo equilibrarlos respecto de los derechos de protección de datos.[56] Los Estados miembros de la UE ya han enfrentado esta obligación durante dos décadas conforme la Directiva de 1995, y muchos no han logrado cumplirla[57]. Algunos países nunca han aprobado las leyes necesarias, mientras que otros han sancionado leyes que no satisfacen por completo el fin de equilibrar los derechos a la libertad de expresión y a la intimidad.[58]

[54] Consejo Asesor de Google, *supra* nota 4.

[55] Art. 17.3.

[56] Art. 85.

[57] Erdos, David. "Fundamentally Off Balance: European Union Data Protection Law and Media Expression", Paper Nº 42/2014, Universidad de Cambridge, Facultad de Derecho, 25 de julio de 2014. Disponible en: http://bit.ly/2fgRXfc.

[58] Id. en 11. "Las leyes de tres países (Croacia, República Checa y España) determinan la no derogación de los medios de ninguna parte del esquema de protección de datos".

Además, algunas protecciones vinculadas al RGPD solo aplican a expresiones periodísticas, artísticas, académicas y literarias. Esta formulación no es exclusiva del derecho de la UE, sino que es un problema para la participación democrática en la comunicación en internet. La mayoría de los usuarios de internet carece de las credenciales para recibir dichas excepciones limitadas. El contenido relevante que quede fuera del alcance de dicha norma podría incluir críticas de los consumidores sobre peligrosas prácticas de negocios y relatos en primera persona de abusos por parte de familiares o personas en posiciones de poder.[59]

El desequilibrio institucional del respaldo gubernamental a los derechos de protección de datos y libertad de expresión en el marco del RGPD provoca más problemas. Un individuo que reafirma sus derechos de protección de datos accede a una audiencia y a un supuesto colaborador en la Agencia de Protección de Datos, que podría dar curso a sus válidos reclamos de manera eficiente y poco costosa. Por el contrario, son pocas las avenidas legales al alcance de un editor o usuario de internet que reclama sus derechos a la libertad de expresión en contra de la eliminación de datos de acuerdo con el derecho al olvido según la legislación europea. Ninguno de los reclamos tiene posibilidades de resolverse con éxito. En la mayoría de los casos, no existe una clara causa de acción contra un individuo cuya acusación falsa haya llevado a un intermediario a eliminar contenido, o contra un intermediario por haber tomado dicha acusación al pie de la letra.

Las desventajas acumuladas del RGPD para los derechos a la libertad de expresión serían relativamente inofensivas si la Ley de Protección de Datos se aplicara principalmente a los datos *back-end* que las empresas manejan y tratan internamente. Sin embargo, aplicar las mismas reglas a la expresión pública en línea de los usuarios de internet los despoja de una protección robusta para su participación y expresión en la web. Las jurisdicciones en América Latina pueden proteger sin afectar los derechos a la protección de datos o a la intimidad de acuerdo con sus propias leyes nacionales.

II.B. Protección procedimental para la libertad de expresión y el

[59] El RGPD no establece claramente quiénes son los sujetos del derecho a la libertad de expresión: los derechos del intermediario o del usuario. Si bien la mayoría de los defensores de la libertad de expresión señalarían al usuario como el sujeto de derecho más importante, la jurisprudencia de la UE, incluido el fallo de "Google Spain", ha analizado en ciertas ocasiones únicamente los derechos de los proveedores de servicios de internet acusados. Véase el análisis sobre la posición para reafirmar los derechos de los usuarios de internet en casos europeos, disponible en: http://stanford.io/2fFmxyG.

derecho al olvido

Una crítica importante del fallo de "Google Spain" fue que efectivamente delegó las decisiones que equilibran los derechos a la intimidad y libertad de expresión de los usuarios en manos de empresas tecnológicas extranjeras, en lugar de delegar dicha responsabilidad en tribunales nacionales. Por supuesto, dichas decisiones ya se encuentran en manos privadas en el marco de muchas leyes vigentes de responsabilidad de intermediarios. Como se analizó anteriormente, las leyes de notificación y baja bien elaboradas pueden nivelar el riesgo de la comunicación en línea mediante la aplicación de controles procedimentales sobre la eliminación excesiva de contenido. Por ejemplo, la Ley de Propiedad Intelectual de Chile establece procedimientos para notificarle al infractor acusado cuando alguien solicita retirar su contenido, y permitirle "contranotificarse" para defenderse de la acusación en cuestión.[60]

La decisión del TJUE sobre Google Spain no determinó ningún proceso en especial para que Google siguiera una evaluación y actuación de los reclamos de derecho al olvido. El Tribunal no hizo referencia alguna sobre leyes de responsabilidad de intermediarios bajo la Directiva sobre comercio electrónico, quizás debido a que se reconoce ampliamente en la UE que dichas disposiciones no cubren la protección de datos.[61] Las opiniones posteriores de los organismos reguladores de protección de datos han agregado mejoras modestas, aunque ninguna se acercó a las fuertes reglas de notificación y baja avaladas por las leyes de responsabilidad de los intermediarios de muchos países.[62] El RGPD introducirá reglas procedimentales que son considerablemente peores, y que reemplazan la incertidumbre existente sobre los esquemas de notificación y baja para el derecho al olvido por un nuevo proceso que carece de las protecciones básicas para la expresión en internet.

El RGPD, una actualización y reforma integral de la Directiva de Protección de Datos de 1995, entrará en vigor el 25 de mayo de 2018. Dado que se trata de un reglamento y no una directiva, no se implementará como ley

[60] Ley No. 20.435, 4 de mayo de 2010, enmienda de la Ley de Propiedad Intelectual, Art. 85U.

[61] Mi próximo artículo analiza la complejidad de la legislación de la UE. El debate surge a partir del texto de la Directiva sobre comercio electrónico, que señala que no aplica a asuntos enmarcados en el artículo 1.5(b) de la Directiva de Protección de Datos.

[62] Guías del Grupo de Trabajo del Artículo 29 sobre la implementación de la sentencia del Tribunal de Justicia de la Unión Europea sobre "Google Spain and Inc. vs. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González C-131/12 (EC)", 14/EN (WP 225), 26 de noviembre de 2014, disponible en: http://bit.ly/1rz3sgx, p. 3, ¶ 9, Art. 17.1.

individual en cada Estado miembro de la UE. Por el contrario, entrará en vigor de forma automática. El RGPD abarca un amplio espectro, con disposiciones que abordan desde la transferencia de datos hasta los códigos de conducta empresarial y la designación de funcionarios de protección de datos.

El RGPD está colmado de ambigüedades, incluso en las disposiciones relativas al derecho al olvido. Algunas perpetúan los planteos existentes y no resueltos conforme la Directiva de 1995, otras son nuevas. Es improbable que pronto contemos con un consenso de expertos respecto de todo lo que significa el RGPD. Una de las ventajas es que promueve los litigios y la incidencia de políticas relativos al impacto que el RGPD tendrá en los intermediarios de internet y la libertad de expresión de los usuarios. En cuanto a las desventajas, las instrucciones no son claras para los intermediarios, junto con fuertes incentivos financieros para entender la interpretación más conservadora de las reglas sustantivas y procedimentales acerca de la eliminación de contenido vinculada al derecho al olvido.[63] Dado que únicamente los intermediarios, no las partes acusadas, conocen la solicitud y pueden participar en los procedimientos de la Agencia de Protección de Datos disminuyen las posibilidades de que las APD y los tribunales revisen las irregularidades y adopten interpretaciones más favorables a la libertad de expresión.

Las reglas de notificación y baja del RGPD surgen de diferentes secciones a lo largo del documento. El análisis más profundo revela un proceso de eliminación como este. Mi próximo artículo y el blog del sitio web Stanford CIS[64] analizan de forma más detallada el proceso del RGPD.

- Una persona física efectúa una solicitud de retiro de información. No existen requerimientos específicos para la información que debe proporcionar la persona a fin de sustanciar su solicitud o confirmar que la misma no presenta conflicto alguno con el interés público.[65]
- El solicitante puede obligar al intermediario a suspender o "restringir" temporariamente el contenido a fin de que no se encuentre disponible para el público mientras el intermediario se encuentra evaluando la solicitud.[66]

[63] Las multas pueden ascender hasta un 4% de la facturación global anual o 20 millones de euros, Art. 83.

[64] Keller, Daphne, "Comentario a la versión final de la legislación europea de 'Derecho al Olvido'", The Center for Internet and Society Blog, Universidad de Stanford, 2 de febrero de 2016, disponible en: http://stanford.io/2fFogE7.

[65] *Véase* Art. 17.1(c) y Art. 12.3-12.6. En contraste, la Ley de Propiedad Intelectual de Chile especifica las formalidades y la información requerida para las solicitudes de retiro de información Ley No. 20.435, *supra* nota 60, art. 85Q.

[66] Art. 18.

- El intermediario analiza el reclamo judicial del solicitante para decidir si el mismo tiene validez. En caso de que tenga dudas importantes, podrá consultar con el usuario que publicó el contenido.[67] El RGPD identifica el derecho a la libertad de expresión como un factor de esta decisión, pero no brinda orientación alguna respecto de su relación con los derechos de protección de datos.[68]
- Para los reclamos válidos, el intermediario procede a "eliminar" el contenido.[69] No hay indicación de que dicha "eliminación" signifique un retiro de datos menor al 100%, aunque el precedente de Google Spain parecería respaldar una acción menos drástica. En cuanto a los reclamos no válidos, el intermediario debería quitar la "restricción" al contenido y volver a instalarlo al dominio público. Aparentemente, no sufre ninguna consecuencia en caso de no volver a restaurar el contenido.
- El intermediario le informa al solicitante sobre el resultado, y comunica la solicitud de eliminación a otros "controladores" que realizan el tratamiento de los mismos datos.[70]
- Si el intermediario tiene información sobre el usuario que publicó el contenido ya retirado, aparentemente, debe notificarle al individuo que solicitó el retiro de los datos.[71]
- En la mayoría de los casos, el publicador acusado no recibe ningún aviso respecto de que su contenido ha sido removido, y no tiene la oportunidad de objetar dicha acción. El texto del RGPD no especifica esta prohibición, pero no hace nada por cambiar la base legal de las conclusiones de los reguladores sobre este punto en el contexto de Google Spain.[72]

En este punto, el desvío del proceso normal de notificación y baja es significativo, y peligroso para los derechos a la libertad de expresión y acceso a la información de los usuarios de internet. Una de las cuestiones principales del proceso de RGPD es el paso 2: la "restricción" inmediata y temporaria del contenido en el dominio público. Existen argumentos que un intermediario podría invocar para omitir este paso en casos especiales,

[67] Esta autorización no está especificada en el RGPD, pero repite el texto de la Directiva de Protección de Datos de 1995, que, según la interpretación de los reguladores, establece dichas normas. Véase Guías del Grupo de Trabajo del Artículo 29, supra nota 62, p. 3, ¶ 9, Art. 17.1.

[68] Art. 17.3.

[69] Art. 17.1.

[70] Art. 17.2 y Art. 19.

[71] Art 14.2(f) y 15.1(g).

[72] Guías del Grupo de Trabajo del Artículo 29, *supra* nota 62, p. 3.

pero no queda claro si dichos argumentos realmente podrían prevalecer, y plantearlos sería un riesgo costoso para los intermediarios. Las disposiciones de restricción marcan un cambio importante: se pasa del supuesto de que la expresión en internet está permitida hasta que se demuestre lo contrario, al supuesto de que el cuestionador tiene la razón. Esto marca un conflicto tanto con las protecciones jurídicas normales sobre libertad de expresión[73] como con nuestro conocimiento sobre las solicitudes vinculadas al derecho al olvido del mundo real. Es importante recordar la tasa del 57% de notificaciones falsas informada por Google. Una acusación realizada en secreto a una empresa privada no debería implicar consecuencias tan dramáticas. El requerimiento de "restricción" del RGPD podría tener sentido al aplicarse a los datos *back-end* almacenados y utilizados por las empresas. Pero en circunstancias donde se aplique el proceso de notificación y baja a las expresiones de los usuarios en internet, dichas expresiones merecen una mejor protección.

El RGPD también genera una injusticia procedimental importante en el paso 6, al impedir al usuario que publicó el contenido en disputa saber qué se ha removido o eliminado del buscador. Sería importante notificarle al usuario afectado a fin de evitar el retiro excesivo de datos en el contexto del RGPD, en particular para los intermediarios más pequeños que poseen escasos recursos legales. Uno de los fines principales de dicha notificación es permitir que los usuarios afectados corrijan los errores de los intermediarios y los errores del notificador.

Las notificaciones que se vuelven rutinarias fomentan un proceso de error y corrección en manos de aquellas personas que estén más motivadas y mejor equipadas para aprovechar la oportunidad, es decir, el publicador del contenido. Dejar la decisión completamente en manos de una empresa de tecnología no puede suplir el hecho de involucrar al publicador como mecanismo para minimizar los retiros inapropiados.

Desde una perspectiva puramente de protección de datos, dejar al publicador acusado fuera del circuito es razonable: si una persona física tiene el derecho a impedir que la empresa continúe con el tratamiento de sus datos, entonces eso también debería evitar que hable con el publicador al respecto. Este razonamiento del tipo "cuando digo basta, quiero decir basta" puede resultar lógico para los datos *back-end* almacenados. Pero cuando el dere-

[73] En el marco de una notable excepción, un fallo anterior a la creación del Marco Civil brasileño sostuvo que una plataforma de internet debía remover temporariamente, dentro de las 24 horas de recibir la notificación, el contenido del usuario, pendiente de un análisis legal del reclamo del notificador. Tribunal Superior de Justicia, Tercer Panel, Google Brasil, apelación especial N° 1.323.754/RJ, 28 de agosto de 2012.

cho a la libertad de expresión de una persona física está en riesgo, impedir sistemáticamente que dicha persona tenga la oportunidad de defenderse es una grave negación a la justicia y al debido proceso.

Por último, es notable el supuesto requerimiento del RGPD de que los intermediarios revelen datos personales sobre personas físicas que enfrentan una acusación. También pareciera ser un artefacto de reglas que apuntan a los datos *back-end*, que enumeran las obligaciones de los controladores cuando alguien les envía información sobre una persona física. Los controladores deben notificarle al sujeto de la información "de qué fuente se originan los datos personales"[74] y "toda información disponible respecto de la fuente".[75] El RGPD no hace referencia alguna a citaciones u otros procesos legales válidos para los controladores que reciben datos de usuarios a fin de proteger los datos personales de dichos usuarios.

Es de suponer que dicha obligación parecerá inadmisible tanto para los reguladores de la privacidad como para los defensores de las libertades civiles, y encontrarán la manera de evitarla. Notablemente, los legisladores latinoamericanos enfrentarían el mismo problema de acuerdo con la legislación actual de protección de datos si siguieran el precedente del caso "Google Spain" y trataran a los intermediarios como controladores de datos de la comunicación de los usuarios. La legislación de Chile, Colombia y, probablemente, otros países exige que los controladores que no pertenezcan al entorno periodístico revelen la fuente de los datos personales.[76]

III. Cuestiones vinculadas al fallo "Google Spain" para los países que no pertenecen a la UE y que consideran las leyes de derecho al olvido

Los avances mencionados en la legislación sobre protección de datos de la UE presentan ramificaciones para los países que están fuera de la UE. Cuando el RGPD entre en vigor, se intensificarán los planteos respecto de seguir los pasos de la legislación de la UE.

Desde una perspectiva de derechos humanos, esta es una cuestión com-

[74] Art. 14.2(f).

[75] Art. 15.1(g).

[76] DLA Piper, Data Protection Laws of the World", 2016, disponible en: http://bit.ly/1rmPSDq

Curiosamente, un tribunal de apelaciones de Chile se basó en una ley de protección de datos como motivo para no revelar información de usuarios en internet en un caso que rechazó la responsabilidad de una plataforma de internet por difamación (Corte Suprema de Chile, *supra* nota 20).

pleja. Por un lado, la legislación de la UE ha sido admirablemente robusta e innovadora para proteger el derecho a la intimidad de los usuarios de internet. Existen buenas razones por las que los defensores quisieran copiar varios aspectos de su contenido. Por otro lado, el modo en que el derecho al olvido se ha desarrollado en Europa pone menos énfasis al derecho a la expresión que muchos otros sistemas jurídicos. Además, en términos de doctrina y ley indiscutible, los avances de la UE fueron impulsados, en parte, por reglas propias de Europa, sin corolario en América Latina. A continuación, se describen las consideraciones pertinentes a las políticas desarrolladas fuera de la UE.

III.A. ¿El fallo de "Google Spain" promueve la misma interpretación de la legislación de otros países, que se asemeje a la Directiva de Protección de Datos?

Por supuesto, los tribunales nacionales tendrán su propia interpretación de las leyes nacionales y no considerarán que el fallo del TJUE es razonable para sus propios países. Pero, en la medida en que el precedente de la UE es relevante, es importante reconocer que la interpretación del TJUE no fue, de ningún modo, una conclusión inevitable, incluso bajo la legislación de la UE. En realidad, el mismo abogado general del TJUE recomendó el resultado contrario: que Google no actuó como controlador y que, en todo caso, la Directiva de Protección de Datos no respaldó el derecho a eliminar información pública según preferencias personales.[77]

Varios especialistas en protección de datos criticaron el análisis del tribunal una vez concluido el caso. Es posible que las críticas basadas en las cuestiones de libertad de expresión sean los fundamentos más importantes para que otros países elijan un rumbo diferente, desde la perspectiva de los derechos humanos. Pero las críticas basadas exclusivamente en la doctrina también son importantes para aquellos países con legislación similar a la de la UE. Por ejemplo, es difícil clasificar a un intermediario como controlador, debido a algunas de las obligaciones principales de este último, las cuales son efectivamente imposibles de cumplir por parte de los intermediarios.

Por ejemplo, los controladores deben obtener un consentimiento o autorización especial antes de tratar datos sobre la salud, la etnicidad, la orientación sexual u otros atributos "sensibles" de las personas. En el caso de plataformas abiertas de expresión que aceptan las declaraciones de los usuarios acerca de

[77] Opinión del defensor general Jääskinen, TJEU, caso C-131/12, "Google Spain SL vs. Agencia Española de Protección de Datos", sentencia del 13 de mayo de 2014, ¶ 20, disponible en: http://bit.ly/2fbElQH.

otras personas, esto resulta imposible.[78] Es absurdo notificar a los interesados antes de "recolectar" datos sobre ellos cuando esta "recolección" consiste en permitir que un usuario libremente divulgue sus ideas en línea.[79]

Estas cuestiones podrían de inmediato respaldar la conclusión legal de que los intermediarios no son responsables del tratamiento del contenido generado por los usuarios. O de otro modo, podría respaldar la conclusión de que se convirtieron en responsables y asumieron la obligación de eliminar la información, solo después de la adecuada y sustancial notificación. La Corte Suprema de Italia llegó exactamente a esta misma conclusión en un caso anterior a "Google Spain".[80] Enmarcar el problema de este modo llevaría a la protección de importantes valores de la intimidad. Preservaría los derechos de protección de datos de toda la comunidad de usuarios de internet en relación con el rastreo *back-end* o la elaboración de perfiles de datos. Y les permitiría a los legisladores aplicar los esquemas vigentes de notificación y baja, incluidos los derechos de libertad de expresión, al discurso en línea de los usuarios.

III.B. ¿Qué es el "derecho al olvido"?

Tal como se mencionó anteriormente, el derecho adoptado por el TJUE en Google Spain se refirió al derecho a ser removido de determinados resultados de búsquedas en la red. La pregunta que aún queda sin responder es si alguna versión de este derecho aplica a otras fuentes de información, incluidos los mismos sitios web. Extender el derecho más allá de los resultados de una búsqueda tendría graves consecuencias. A medida que los defensores consideran las propuestas sobre el derecho al olvido en otros países, es esencial delinear el alcance de las expresiones en internet y fuera de ella, que puedan verse afectadas por ese derecho.

III.C. ¿La Ley de Responsabilidad de los Intermediarios debería influir en las consideraciones del derecho al olvido fuera de la UE?

La asociación entre la Ley Convencional de Responsabilidad de los Intermediarios y la práctica de notificación y bajas del derecho al olvido es simple

[78] *Véase* análisis en Peguera, *supra* nota 53.

[79] Varias leyes de protección de datos latinoamericanas, que incluyen la de México, Colombia y Argentina, poseen versiones de este requisito. DLA Piper, *supra* nota 76.

[80] Corte Suprema de Italia, "Milan Public Prosecutor's Office vs. Drummond", 5017/14, sentencia del 12 de diciembre de 2013, disponible en: http://bit.ly/2efrUYY ¶ 7.4 (traducción informal).

en términos conceptuales. Las consideraciones sobre la libertad de expresión son las mismas desde la perspectiva del usuario afectado, independientemente del marco jurídico que suprima su discurso. Sin embargo, en Europa existe una importante barrera jurídica que complica esta situación. La Directiva de Comercio Electrónico, que rige todos los demás aspectos de la responsabilidad de los intermediarios en la UE, establece que "esta Directiva no aplicará a cuestiones relacionadas con los servicios de la sociedad de la información incluidos en la Ley de Protección de Datos"[81]. Esto lleva a que muchos abogados de la UE, si bien no todos, concluyan que el derecho al olvido recae fuera de las reglas comunes de notificación y baja. Esa excepción, de existir, es puramente europea. No debería impedir que otros países fuera de la UE elaboraran sus propias leyes de responsabilidad de los intermediarios.

Un asunto más complejo es si la obligación de los responsables de suprimir los datos personales es una verdadera forma de "responsabilidad" del contenido de terceros, o si se trata, en cambio, de su propia obligación. Pero esta cuestión también está sujeta a diferentes leyes y consideraciones en los distintos países. Para la jurisprudencia que da marco a las reglas de responsabilidad de los intermediarios como una forma de proteger la expresión, existen escasos motivos para cambiar dicha protección dependiendo de las concepciones legales de "responsabilidad".

III.D. ¿El análisis del TJUE sobre los derechos fundamentales es coherente con las obligaciones de derechos humanos y el derecho constitucional en mi país?

El TJUE sugirió que el derecho a la intimidad o a la protección de datos debería, "a modo de regla", prevalecer por sobre los derechos de acceso a la información de las personas. Esta conclusión fue ampliamente criticada por abogados de la UE, pero representa una ley para la eliminación de datos en el marco del derecho al olvido como en Google Spain. Esta priorización del derecho a la intimidad por sobre el derecho a la expresión es sin dudas incorrecta en algunos otros sistemas, incluido el sistema interamericano de derechos humanos. Esa diferencia resulta pertinente para las dos cuestiones sobre la libertad de expresión del derecho al olvido: el alcance del derecho sustantivo y las reglas procedimentales para las empresas de internet que ofician como adjudicadoras de la expresión en la web. También, podrían surgir diferencias a partir del modo en que las constituciones nacionales

[81] Directiva de Comercio Electrónico, Artículo 5.1(b). *Véase* también, Considerando 14.

definen y delinean los derechos. La protección de datos, como un derecho distinto del derecho a la intimidad, constituye un derecho fundamental de la Carta de la UE. Los expertos latinoamericanos en países con derechos constitucionales de *habeas data*[82], y en países donde únicamente los derechos tradicionales a la intimidad se encuentran protegidos en sus constituciones, deberán enfrentar importantes interrogantes para equilibrar estos derechos de acuerdo con sus propios sistemas constitucionales.

III.E. ¿La legislación nacional vigente protege los derechos a la intimidad y a la dignidad en internet?

En el caso de las leyes vigentes que les otorgan a las personas los instrumentos necesarios para proteger su intimidad, buen nombre, dignidad y honor, o para evitar la discriminación basada en la información personal, es importante preguntarse qué aportaría la adopción del derecho al olvido[83]. Agregar legislación nueva y confusa sobre el derecho al olvido, sin vincularla a los distintos grados de denuncias y defensas de las leyes vigentes, solo embarraría las aguas y aumentaría las denuncias frívolas y el retiro excesivo del contenido en internet.

Si los legisladores observan fallas en las leyes existentes, se podría resolver con leyes más personalizadas que incluyan la protección a la libertad de expresión, sin invocar el terminante instrumento de las leyes sobre derecho al olvido similares a las de la UE.

III.F. ¿La UE ya aplica su Ley de Protección de Datos a la expresión en internet en mi país?

En el caso de Google Spain, uno de los principales fallos fue jurisdiccional. La ley de la UE se aplicó al tratamiento de datos realizado fuera de Europa por parte de la empresa matriz estadounidense Google, debido a las conexiones entre la búsqueda en la red y las ventas por publicidad llevadas a cabo por la subsidiaria local. Muchos expertos sostienen que la Directiva de 1995 también aplica a empresas extranjeras sobre la base de otros fundamentos.

Cualquiera sea la respuesta según esa ley, el RGPD claramente expande

[82] Esto incluye, con algunas variaciones a Argentina, Brasil, Colombia, México, Perú y Venezuela. Cerda Silva, *supra* nota 3.

[83] Keller, Daphne y Brown, Bruce D., "Europe's Web Privacy Rules: Bad for Google, Bad for Everyone", *The New York Times,* 25 de abril de 2016, disponible en: http://nyti.ms/2fpm3f2.

la aplicación extraterritorial a las empresas de internet en todo el mundo, incluso a aquellos encargados de procesar y controlar la información, siempre y cuando "monitoricen" a los usuarios de la UE.[84] El término "monitorizar" parece comprender las cuentas en internet y las funcionalidades comunes de personalización de red y de aplicaciones, por lo que la ley alcanza a muchas empresas de internet fuera de la UE. Además, los reguladores han ratificado que dichas empresas deberán suprimir el contenido en todo el mundo, incluso en aquellos países en donde el contenido esté protegido por leyes de libertad de expresión. Esta aseveración sobre la jurisdicción coloca a empresas extranjeras y a legisladores extranjeros en una posición incómoda, ya que deben lidiar con cuestiones de adherencia y manejar las relaciones diplomáticas y comerciales en la UE.[85]

En la práctica, los reguladores de la UE probablemente no prioricen o dediquen recursos al control de empresas pequeñas y distantes. Pero el RGPD será un problema para las empresas que tengan una creciente base de usuarios de la UE y presencia en Europa.[86] Deberán pensar mucho sobre sus obligaciones de acuerdo con el reglamento en general, no solo sus requisitos sobre el derecho al olvido. (Existe una pregunta interesante acerca de la autoridad que transita en un rumbo opuesto: ¿las leyes sobre el tratamiento de datos, que no son de la UE, incluidas las reglas potencialmente más liberales que equilibran la libertad de expresión, deberían regir el tratamiento europeo?).

III.G. ¿Las agencias administrativas pueden adjudicar derechos de libertad de expresión bajo el marco jurídico de mi país?

Al ampliar la Ley de Protección de Datos para incluir la expresión pública en internet, el fallo de "Google Spain" delegó la autoridad a manos de los reguladores de la protección de datos. Estas agencias administrativas pueden decidir si será posible buscar determinada información mediante motores de

[84] Art. 3.2(b).

[85] *Véase*, Keller y Brown, supra nota 83.

[86] Otra cuestión jurisdiccional hace referencia a las entidades extranjeras que "ofrecen bienes o servicios" en la UE. Sin embargo, en un considerando, este fundamento queda confinado en base a factores como la moneda nacional que se utiliza para los precios (R. 23). Los considerandos en el RGPD también demuestran una verdadera frustración con denuncias a las que la ley de la UE no alcanza en cuanto a empresas matrices extranjeras de subsidiarias establecidas en la UE, donde indican que "la forma legal de dichos acuerdos, ya sea mediante una filial o una subsidiaria con personería jurídica, no es el factor determinante" para determinar la jurisdicción de "establecimiento", según el artículo 3.1.

búsqueda. Si el derecho al olvido se extiende a las plataformas de hosting, serán los mismos reguladores quienes determinarán si la expresión aparecerá o no en la red. Delegar dicha facultad a las agencias administrativas en lugar de delegarla en los tribunales puede permitirse bajo el marco legislativo y de derechos humanos de la UE. Sin embargo, los formuladores de políticas en otros países pueden llegar a otras conclusiones.

Conclusiones y recomendaciones

Fundamentar el derecho al olvido en una ley de protección de datos similar a la de la UE conduce al desequilibrio en las reglas, que dejan sin protección suficiente a los derechos de libertad de expresión de los usuarios de internet. Una posible solución en la UE y en otras partes sería incorporar nuevas e importantes protecciones sustantivas y procedimentales a la expresión dentro de la Ley de Protección de Datos. Sin embargo, un abordaje más simple sería reconocer que las obligaciones de los intermediarios de suprimir el discurso en la red son muy distintas de las obligaciones que ellos tienen de suprimir los datos *back-end* del usuario. Los problemas que surgen de la eliminación de datos y la necesidad de contar con reglas procedimentales que nos protejan del exceso de eliminación son abordados en las leyes de responsabilidad de los intermediarios y en la jurisprudencia de libertad de expresión. Esas reglas pueden aplicarse para proteger tanto el derecho a la expresión como el derecho a la intimidad y protección de datos.

Los legisladores que se preocupan por proteger todo el espectro de derechos tienen muchas opciones doctrinales en su propia legislación nacional. Si bien varían de un país a otro, las recomendaciones identificadas en este artículo pueden contribuir a que legisladores y defensores de derechos humanos lleguen a marcos jurídicos sólidos a fin de proteger los derechos de los usuarios de internet.

Capítulo Seis

¿Derecho al olvido en el ciberespacio? Principios internacionales y reflexiones sobre las regulaciones latinoamericanas

Nelson Remolina Angarita[1]

¿Tienen derecho las personas a cambiar su vida,
sin que las persiga eternamente el fantasma de la información
negativa de su pasado que ha sido difundida en internet?
Nelson Remolina Angarita

Introducción

La expresión "derecho al olvido" surgió jurisprudencialmente hace varias décadas. En el caso de la República de Colombia, por ejemplo, se analizó por primera vez el 16 de junio de 1992 con ocasión de la sentencia T-414 de la Corte Constitucional[2]. Por mucho tiempo, el tema se centró en la situación de personas que han sido reportadas como deudoras morosas o sujetos que han cometido delitos. Durante el siglo XX se estudió el tema como una cuestión del derecho a la información, el buen nombre y la dignidad humana frente a sujetos determinados como las centrales de riesgo crediticio y el Estado.

No obstante, el debate de los inicios del siglo XXI se ha visto enriquecido con nuevos elementos y circunstancias. De una parte, se han agregado otros elementos como internet y la libertad de expresión. Adicionalmente, el

[1] Nelson Remolina Angarita es profesor asociado de la Universidad de los Andes (Bogotá, Colombia), director del Grupo de Estudios en Internet, Comercio electrónico, Telecomunicaciones e Informática (GECTI) (http://gecti.uniandes.edu.co/2014) y del Observatorio Ciro Angarita Barón sobre la protección de datos personales en Colombia (http://habeasdatacolombia.uniandes.edu.co). Doctor *Summa Cum Laude* en Ciencias Jurídicas de la Pontificia Universidad Javeriana. Master of Laws, The London School of Economics and Political Sciences. Especialista en Derecho Comercial y Abogado (1994) de la Universidad de los Andes (Bogotá, Colombia). Este texto solo refleja la opinión del autor. Email: nremolin@uniandes.edu.co.

[2] *Cfr*. Corte Constitucional, sentencia T-414 del 16 de junio de 1992. MP. Dr. Ciro Angarita Barón. El texto se puede consultar en: http://bit.ly/2f2Pg4v.

derecho al olvido puede ejercerse frente a sujetos indeterminados como lo serían, en principio, cualquier persona que publique información en internet.

El debate del siglo XXI ha tenido como punto de referencia lo sucedido en Europa a partir del fallo del caso Costeja por parte del Tribunal de Justicia[3] de la Unión Europea en 2014. Sin embargo, no debe perderse de vista que mientras en la sentencia de 1992 de la Corte Constitucional de la República de Colombia se hizo alusión explícita a dicho derecho, en la precitada decisión judicial del Tribunal de Justicia no se analizó expresamente el derecho al olvido. No obstante, este último fallo judicial ha sido el referente que generó una cascada de comentarios, artículos y reacciones que han capturado la atención de la academia, las empresas y de los reguladores.

Recientemente, por ejemplo, dicho derecho fue incorporado expresamente en Costa Rica (derecho al olvido), Nicaragua (derecho al olvido digital) y el artículo 17 del Reglamento[4] General de Protección de Datos Personales (RGPDP) del Parlamento Europeo y del Consejo con el nombre de "Derecho de supresión («el derecho al olvido»)", el cual se anuncia como una de las novedades de ese Reglamento.[5]

La construcción jurisprudencial del derecho al olvido ha comprendido el análisis de varios derechos y principios. Dentro de los primeros se mencionan, entre otros, la intimidad, la protección de datos personales, el buen nombre, la libertad de expresión, el derecho a informar y ha recibir información. Dentro de los segundos, se encuentran el principio de la dignidad humana y la neutralidad tecnológica de internet.

El reconocimiento del derecho al olvido es principalmente casuístico. Los hechos reales y las situaciones concretas han sido determinantes para el reconocimiento y garantía del mismo. También ha sido interesante determinar ¿cómo garantizar el derecho al olvido en internet? Es decir, ¿a través de qué medidas se procurará que cierta información negativa no sea conocida por terceros en

[3] *Cfr*. Tribunal de Justicia (Gran Sala). Sentencia del 13 de mayo de 2014. Asunto C131/102. Google Spain, S.L., Google Inc. Y Agencia Española de Protección de Datos (AEPD), Mario Costeja González. El texto puede consultarse en: Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González. El texto del fallo puede consultarse en: http://bit.ly/2a332A6.

[4] *Cfr*. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

[5] *Cfr*. Parlamento Europeo. Reforma de la protección de datos, "Nuevas reglas adaptadas a la era digital" (nota de prensa). Publicada el 14 de abril de 2016 en: http://bit.ly/1XxhgJc.

el ciberespacio? En línea con lo anterior, se han utilizado varios mecanismos que van desde la eliminación de la información hasta la "des indexación", la anonimización, las herramientas técnicas "robots.txt", "metatags" u otros similares que impidan conocer la información que se quiere dejar en el olvido.

Visto lo anterior, este artículo tiene varios propósitos, a saber: (1) destacar la importancia del derecho al olvido y su relación con la dignidad humana; (2) evidenciar el reto que tienen las personas y las autoridades para garantizar el derecho al olvido en el ciberespacio; (3) recalcar que el derecho al olvido es una acepción del derecho de supresión y una concreción del derecho de oposición desde la perspectiva del régimen jurídico del derecho a la protección de datos personales, y (4) precisar que los motores de búsqueda son los principales responsables del tratamiento de datos personales en el mundo y que la indexación de información es el principal detonante de la difusión masiva de la misma en internet.

Nuestras conclusiones no son inmunes a la crítica, la cual es bienvenida. De hecho, puede escribirse un texto con puntos de partida y de llegada totalmente contrarios a los del presente escrito. Eso es natural porque sobre el mismo punto existen diferentes perspectivas (empresariales, académicas, de política pública, entre otras) e intereses (económicos, garantistas de derechos humanos).

Dado lo anterior, nuestras reflexiones iniciales son una mera invitación académica para seguir estudiando más casos a la luz de las particularidades de cada situación fáctica, así como de las herramientas jurídicas y de los fallos judiciales o decisiones administrativas de cada país.

I. El ciberespacio como escenario retador de la garantía efectiva del derecho al olvido

El nivel de garantía efectiva del derecho al olvido depende, entre otras, del contexto en donde se pretende proteger. Este puede ser, por ejemplo, físico, local, electrónico e internacional según el caso. No es lo mismo tratar de ejercer el derecho al olvido frente a una central de información de riesgo crediticio local, o ante un periódico físico, que ejercitar dicho derecho ante cualquier persona –"internauta"– o empresa que publica información sobre otros en internet. En el primer caso, es más viable lograr identificar los responsables y suprimir definitivamente la información que se pretende eliminar a través del derecho al olvido. En el segundo caso, es muy difícil conseguir la "desaparición" definitiva de la información en internet, entre otros, porque la misma puede ser publicada o replicada en la red por millones de personas, o por la complejidad y el desconocimiento del cambiante e innovador mundo tecnológico, el cual

no alcanza a ser entendido por muchos de nosotros, por algunos jueces, funcionarios públicos o reguladores. Por eso, brevemente, queremos referirnos a ciertas cuestiones del ciberespacio e internet que, en nuestra opinión, refleja la sociedad y la realidad del siglo XXI que debemos afrontar.

I.A. Del ciberespacio e internet

Somos testigos de la migración del mundo físico y fronterizo al "ciberespacio", el cual se caracteriza por ser tecnológico y sin fronteras geográficas. Vivimos en un planeta fraccionado en territorios cuya mayoría de actividades se rige por regulaciones nacionales y autoridades con competencia territorial[6] (no transfronteriza). Al mismo tiempo, observamos un proceso de erosión y de desintegración de las fronteras territoriales y la aparición de un espacio de enorme magnitud donde progresivamente aumenta el número de personas que interactúan en el ciberespacio.

El ciberespacio ha sido caracterizado por ser un escenario global no delimitado por fronteras geográficas[7] en donde las actividades suceden dentro de la arquitectura tecnológica de internet que está en plena eclosión de crecimiento desde la perspectiva del número de usuarios. Acá no existe un espacio físico definido (como nuestra casa o el territorio de nuestro país), sino un campo artificial o virtual e indeterminado en donde las personas interactúan. Buena parte de la interacción en el mundo virtual tiene implicaciones y consecuencias jurídicas en el mundo real.

Aunque existen diferentes acepciones sobre el ciberespacio, consideramos relevante tener presente que el mismo está integrado por los siguientes elementos:[8]

- Una infraestructura tecnológica (recursos tecnológicos) conformada por un sinnúmero de equipos (servidores, computadores, teléfonos móviles, tabletas, entre otras) que se encuentran ubicados en muchas partes del mundo.
- Una plataforma de comunicaciones (red global de comunicaciones),

[6] Puede afirmarse que el mundo jurídico actualmente es una amalgama de: (i) reguladores locales con campo de acción definido por un territorio; (ii) regulación fundada en bases territoriales, y (iii) soluciones de controversias normalmente a cargo de jueces o autoridades con competencia delimitada por un territorio.

[7] *Cfr*. Gilden, Michael, "Jurisdiction and the Internet: the Real World Meets Cyberspace, en: *ILSA Journal of International & Comparative Law*, No. 7 (1), 2000, p. 150.

[8] Sobre algunas características del ciberespacio y los retos que genera al derecho véase: Johnson, David y Post, David, "Law and Borders: the Rise of Law in Cyberspace", en: *Stanford Law Review*, No. 48, 1995-1996, pp.1.367-1.402.

información y redes interconectadas (internet) de alcance mundial denominada "infraestructura global de información".[9]

- Millones de personas de diversas nacionalidades, domiciliadas en países con sistemas jurídicos disímiles que desde cualquier parte del mundo hacen uso de la tecnología, las comunicaciones y la información para interactuar con otras personas o utilizar los servicios disponibles en internet.

Internet[10] es la parte técnica del ciberespacio que conecta los "cibernautas" de todas partes del mundo. Se ha planteado que internet es la "red mundial que permite interconectar el mundo entero"[11] en la cual pueden conectarse todas las computadoras y dispositivos móviles del mundo para poner de presente su campo de acción universal y la naturaleza internacional de muchas de las actividades que suceden en internet.

La Internet Society[12] señala que "internet es a la vez una herramienta de emisión mundial, un mecanismo para diseminar información y un medio para la colaboración y la interacción entre personas y sus ordenadores, sin tener en cuenta su ubicación geográfica". Agrega dicha organización que "internet, como la conocemos hoy en día, es una infraestructura de información muy difundida".[13] En otras palabras, internet, cada vez más, tiene

[9] Reidenberg se refiere a ella como "*the global information infrastructure* –GII–" (Reidenberg, Joel R., "Governing Networks and Cyberspace Rule-making", en: *Emory Law Journal*, No. 45, 1996, p. 912.)

[10] Según el *Diccionario de la Lengua Española*, internet es una "red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación", Real Academia Española. *Diccionario de la Lengua Española*. Avance de la 23ª edición. Disponible en: http://bit.ly/2flwznS.

[11] Cassin, Bárbara, *Googléame: la segunda misión de los Estados Unidos*, V. Goldstein (trad.), Buenos Aires, Fondo de Cultura Económica, Biblioteca Nacional, Tezontle, 1ª ed. en español, 2008, p. 15.

[12] La Internet Society es un organización fundada en 1992 cuya misión es "promover el desarrollo abierto, la evolución y el uso de internet para beneficio de todas las personas del mundo" (Internet Society. Misión. http://bit.ly/2aulrT6). Se autodefine como una "organización global unida por una causa común y regida por una variada junta de fideocomisarios dedicada a asegurar que internet siga siendo abierta, transparente y definida para que todos podamos disfrutar de ella" (*cfr*. Internet Society, "¿Quiénes somos?". http://bit.ly/2fO66TR). La Internet Society cuenta con un consejo asesor conformado por académicos, investigadores, proveedores de servicios, equipos y contenidos, entidades gubernamentales, organizaciones internacionales y grupos de interés público (*cfr*. Internet Society, Consejo Asesor. http://www.internetsociety.org/es/consejo-asesor).

[13] Leiner, Barry, Cerft, Vinton y otros, "Breve historia de internet", Internet Society, 1997. http://bit.ly/1jhArXl. Todos los autores de este texto son: Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff.

el don de la ubicuidad en la medida que está presente al mismo tiempo en casi todas partes del mundo.

I.B. Los motores de búsqueda como los principales responsables de tratamiento de datos personales en el mundo

Los motores de búsqueda realizan tratamiento masivo, global y transfronterizo de datos personales de trillones de personas en el mundo. Efectúan muchas operaciones sobre los datos personales como, entre otros, encontrarlos en internet, indexarlos, analizarlos y, en general, usarlos para diversos fines. Por eso, no existe duda que los motores de búsqueda son responsables de tratamiento de datos personales.

En ese sentido, la autoridad colombiana de protección de datos, por ejemplo, concluyó que la indexación que realizan los citados motores hacen parte del tratamiento de la información en comento. En efecto, la Superintendencia de Industria y Comercio mediante concepto del 3 de marzo de 2016 precisó que el tratamiento de datos personales comprende "la recolección, el almacenamiento, la *indexación*, la conservación, el *análisis*, el *uso*, la circulación, la transmisión, la transferencia, la *divulgación*, el *acceso*, la consulta, la supresión y la depuración de datos personales".[14] Con esto, no queda duda que los motores de búsqueda tratan datos personales y por ende deben ser respetuosos de los deberes que les imponen las regulaciones como responsables del tratamiento de enormes cantidades de datos de trillones de personas de todas partes del mundo.

I.C. La indexación como el hecho generador de la multiplicación ilimitada de los datos personales en el ciberespacio

Los motores de búsqueda no son los creadores de la información que publican terceros (como los medios de comunicación o cualquier cibernauta), pero sí son los principales responsables del mundo en difundir masiva e instantáneamente la información que existe en internet. La indexación es el hecho generador de la difusión ilimitada de los datos personales en el ciberespacio. La indexación la hemos asumido como algo "bueno" o por lo menos "normal", la pregunta es ¿por qué la desindexación es algo "malo" o "anormal"?

[14] La cursiva nos pertenece. Sobre este concepto véase: Remolina Angarita, Nelson, "Autoridad colombiana de protección de datos concluye que sí es competente para investigar a Facebook", 2016. Disponible en: http://bit.ly/2gGzmh5.

La indexación es el detonante de la multiplicación ilimitada de los datos personales en la red. Por eso, la desindexación es la medida sensata para mitigar los efectos que ocasiona la indexación respecto de la difusión de información negativa sobre la cual es procedente el derecho al olvido. Ignorar los efectos multiplicadores y globales de los motores de búsqueda y de la indexación es como desconocer que existe internet.

Con la desindexación no desaparece la información publicada, pero la ubicación de esa información no será tan fácil y rápida gracias a la intervención del motor de búsqueda. Por eso, no se deben desconocer los efectos masivos de difusión instantánea y global que generan los motores de búsqueda para encontrar y organizar información sobre una persona en cuestión de segundos.

Si los motores de búsqueda no indexaran la información disponible en internet, no sería tan fácil conocer los datos personales de cualquier persona. ¿Será que no es sensato pedirle a quien "indexa" y facilita la difusión de la información en internet, que "desindexe" y ayude a impedir que se conozca cierta información negativa en casos concretos?

Estamos de acuerdo con la importancia y la necesidad de garantizar la libertad de expresión en internet, pero no debe olvidarse que esa libertad no es absoluta y que la misma debe de analizarse a la luz de los hechos particulares de cada caso, teniendo en cuenta su coexistencia con otros derechos como, entre otros, la protección de datos[15]. Sobre este punto, vale la pena traer a co-

[15] Sobre este punto, nos parece importante la siguiente reflexión de la autoridad peruana de protección de datos: "Lo que se ha ordenado es el bloqueo de los datos personales (nombres y apellidos) del reclamante de toda información o noticia relacionada con la materia de sobreseimiento de la causa N° 39452-2009 (305-09)-CMV que aparece en los resultados del motor de búsqueda Google Search, entendiendo por bloqueo, en este caso, realizar el tratamiento de las publicaciones de forma que se impida que estén disponibles para sucesivos tratamientos de búsqueda e indexación con el criterio de búsqueda nominal.

"Es decir ningún usuario de internet está impedido de acceder a los contenidos alojados en las URLS de los sitios web en internet que se han detallado en la reclamación cuando utilicen el motor de búsqueda Google Search, pero solo podrán llegar a dichos contenidos en la medida que empleen otros criterios de búsqueda que no sean los nombres y los apellidos del reclamante. En consecuencia, la DGPDP considera que:

"La alusión a la libertad de expresión de administradores o webmaster de sitios web en internet resulta impertinente, porque se mantiene inalterada la información materia de reclamación en las páginas web fuente.

"La alusión a la libertad de información de los usuarios de internet, es también impertinente, porque se mantiene la accesibilidad a la información materia de reclamación por el uso de otras palabras en los criterios de búsqueda (conceptos, hechos, materia, número de resolución, fechas, entre otros)" (República del Perú, Resolución Directoral N° 026-2016-JUS/DGPDP del 11 de marzo de 2016. Disponible en: http://bit.ly/2fBFWR6).

lación la siguiente afirmación de la autoridad peruana de protección de datos:

> Ahora bien, como quiera que el derecho fundamental a la protección de datos personales tiene la misma jerarquía que cualquier otro derecho fundamental no se admite que, en general y en abstracto, otro derecho deba considerarse por encima de él. La ponderación y la evaluación deben hacerse en cada caso concreto.
> En efecto, la libertad de expresión coexiste con otros derechos, y nuestra obligación es proteger uno de esos derechos, ya que ningún derecho fundamental deberá servir para afectar a otro derecho fundamental, de forma que el establecimiento de límites entre uno y otro no debe presentarse, como pretende la recurrente, como una cuestión de "conflicto" o "incompatibilidad", sino como la delimitación de las formas de "coexistencia" de ambos derechos. De manera que los argumentos en favor de la libertad de prensa pueden ser ciertos y abundantes, pero en forma alguna justifican la anulación del derecho a la protección de datos personales[16].

Desindexar no es una modalidad de control previo, sino una forma de solucionar problemas que ocasiona, entre otras, la indexación masiva e indiscriminada de información en internet. Desindexar no significa que el motor de búsqueda sea responsable del contenido. Al indexar la información el motor de búsqueda facilitó su difusión y ubicación. Por eso, en casos justificados es procedente que se desindexe para que el motor deje de facilitar la difusión de información negativa que afecta a una persona.

La desindexación es una medida sensata para poder ayudar a que se olvide cierta información negativa con miras a garantizar algunos de los derechos humanos de las personas y, en últimas, reivindicar la dignidad humana en casos concretos.

I.D. El "internet de las empresas" (Internet of Corporations) y la protección de los derechos humanos en el ciberespacio

El "internet de las empresas"[17] o "*Internet of Corporations*" (IoC) es otra

[16] República del Perú, Resolución Directoral N° 026-2016-JUS/DGPDP del 11 de marzo de 2016. Disponible en: http://bit.ly/2fBFWR6.

[17] Esta sección retoma parte del siguiente artículo del autor. Ver: Remolina Angarita, Nelson, *"Internet de las empresas" ["Internet of Corporations" –IoC–]: una explicación de lo que pasa en internet y del futuro de la protección de los derechos humanos en el ciberespacio (Parte 1)*, publicado el 28 de junio de 2016 en http://bit.ly/2gi9wfl.

expresión que sugiero tener presente tal y como se ha hecho con el "internet de las cosas" *(internet of things)*. No se trata de un tema menor porque, en mi opinión, el "internet de las empresas" sintetiza, en gran parte, lo que ha ocurrido con la regulación de internet. El "internet de las empresas" ha fijado el destino de internet y de sus usuarios porque ha sido hiperregulado por las empresas, quienes utilizan sus "notas legales" o sus "términos y condiciones" para establecer las reglas que, a julio de 2016, rigen el destino de más de 3,42[18] billones de personas de todas partes del mundo.

El "internet de las empresas" hace referencia a las normas que los empresarios han creado para realizar negocios o prestar servicios en internet. Se trata de las pautas que los comerciantes consideran sensatas bajo su modelo de negocios para ganar utilidades. En últimas, se trata del internet que las empresas desean que sea, para ganar dinero. Estas regulaciones podríamos denominarlas como las **"leyes empresariales"**, las cuales hacen parte de las normas corporativas vinculantes o binding corporate rules (BCR). Dichas normas son las que a mediados de 2016, por ejemplo, rigen a más de 1,70 billones de usuarios de Facebook,[19] o a las personas que diariamente realizan más de 2,85 billones de búsquedas en Google[20] y, en general, a los seres humanos que acceden a un poco más de 1,05 billones de páginas web[21] disponibles en internet.

Como se observa, estamos frente a una realidad de enorme magnitud que involucra la "economía digital" y la protección efectiva de los derechos humanos de trillones de personas en internet. Todo lo anterior también evidencia el "poder en internet" y la "fragilidad de la protección de los derechos humanos en el ciberespacio" porque, en la práctica, el alcance de los derechos humanos en internet depende, en gran parte, de lo que definen las leyes empresariales. Piénsese, por ejemplo, lo siguiente: ¿La empresa dueña de un motor de búsqueda acepta o no el reconocimiento del derecho al olvido? En caso positivo, la persona no tendría dificultades para que su información se desindexe. Pero si la empresa no está de acuerdo con el derecho al olvido, entonces la persona tendrá que acudir a las autoridades locales para alcanzar dicho cometido y obligar al motor de búsqueda que desindexe la información como un mecanismo para proteger los derechos de la persona en una situación concreta.

El "internet de las empresas" ha colonizado gran parte de las actividades en internet. Frente a esa colonización, los Estados han expedido leyes que

[18] *Cfr*. http://bit.ly/1cWKuda. Último acceso: 29 de julio de 2016.
[19] *Cfr*. *Ibíd*.
[20] *Cfr*. *Ibíd.*
[21] *Cfr*. *Ibíd*.

inciden en las actividades que realizan las empresas en internet. Dichas regulaciones estatales han surgido por varios motivos como, entre otros, los siguientes: la protección de los intereses generales, la protección de los derechos humanos de sus ciudadanos, la protección de los consumidores del comercio electrónico. Muchos de los objetivos de la regulación estatal quedaron resumidos en la declaración conjunta sobre comercio electrónico de los Estados Unidos y Europa del 5 de diciembre de 1997.[22]

Los fines de las empresas y los objetivos de los Estados explican los propósitos de las reglas de cada uno. Mientras la finalidad de una empresa es ganar dinero, la misión del Estado es, en términos generales, "servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución".[23] Los objetivos de las empresas están redactados en sus estatutos sociales y son definidos unilateralmente por el empresario, mientras que las finalidades del Estado están definidas en las Constituciones de cada país y son acordadas democráticamente.

Como se observa, son diversos los propósitos de las empresas y las finalidades de los Estados. No obstante, unos y otros no son excluyentes. Los negocios y la debida protección de los derechos humanos son asuntos de gran importancia para algunas empresas. Lo mismo sucede con la innovación y los derechos humanos.

El *big data*, la computación en la nube *(cloud computing)* y el internet de las cosas *(internet of things)* son creaciones del "internet de las empresas". Detrás de cada uno existe un modelo de negocio que apunta a obtener dinero, lo cual es legítimo. El punto a determinar es, entre otros, el siguiente: ¿Son consistentes las leyes empresariales con los mandatos constitucionales y los documentos internacionales en materia de derecho humanos? ¿Es suficiente lo que hacen las empresas para garantizar los derechos de las personas en internet? ¿Las empresas extranjeras que realizan negocios en internet, respetan las normas locales sobre derechos humanos que emiten los Estados? ¿Las empresas extranjeras que realizan negocios en internet y que no están domiciliadas en determinado país, deben colaborar con las autoridades locales de ese país para hacer efectiva la protección de los derechos de las personas en internet? ¿Las empresas extranjeras que realizan negocios en internet y que no están domiciliadas en determinado país, deben cumplir las instrucciones de las autoridades locales de ese país para hacer efectiva la protección de los derechos de las

[22] El texto de la declaración puede consultarse en: http://bit.ly/2ggzjW6.

[23] *Cfr*. Artículo 2 de la Constitución de Colombia.

personas en internet? ¿Las empresas extranjeras que efectúan negocios en internet deben someterse a las leyes locales, o las autoridades nacionales deben someterse al "internet de las empresas"?

Las anteriores son preguntas de gran importancia para el futuro de la protección de los derechos y sobre las cuales algunas autoridades han empezado a pronunciarse. En un caso reciente, por ejemplo, la Autoridad de Protección de Datos de la República del Perú concluyó que:

> Admitir los argumentos de defensa de la empresa Google –bajo la personería de Google Inc. o de Google Perú S.R.L.– supondría admitir que puede desplegar sus actividades en territorio peruano, usar medios peruanos, tratar información de ciudadanos peruanos y comercializar publicidad para el mercado peruano, al margen de lo que ordenan la Constitución Política del Perú, la LPDP y su reglamento, sobre el derecho que todos y cada uno de los ciudadanos peruanos tenemos a que se protejan nuestros datos personales.[24]

I.E. Del reto de la protección efectiva de los derechos en el ciberespacio

En 2001 la Corte Constitucional de la República de Colombia se pronunció sobre, entre otros, el alcance del ordenamiento constitucional frente a la regulación de materias ligadas al ejercicio de actividades a través de internet.[25] Para la Corte la información es muy importante y cumple un rol central "en el funcionamiento de la sociedad actual" e internet ha sido, entre otros, un escenario en el cual operan muchos "sistemas de información y almacenamiento informático". De entrada, la Corte declaró rápidamente que:

> La información que se comparte en internet deja una huella que, (…) hace posible rastrear e identificar todo lo que una persona hizo en el mundo virtual, los lugares que visitó o consultó y los productos que consumió a través de la red. La recopilación de estos datos puede ser utilizada para crear perfiles sobre los gustos, preferencias, hábitos de consulta y consumo de las personas que emplean internet (como simples usuarios o como agentes económicos que desarrollan sus

[24] *Cfr*. República del Perú, Resolución Directoral N° 026-2016-JUS/DGPDP del 11 de marzo de 2016. Disponible en: http://bit.ly/2fBFWR6.

[25] *Cfr*. Corte Constitucional, sentencia C-1147 del 31 de octubre de 2001, MP, Dr. Manuel José Cepeda Espinosa.

actividades por este medio).[26]

Por otra parte, la Corte también reconoció la importancia "que tienen dentro de un sistema global de comunicaciones, como internet, derechos y libertades tan importantes para la democracia como (….) la intimidad y el habeas data (artículo 15 C.P.)".[27] Adicionalmente, dicha corporación admitió que los avances científicos y tecnológicos "*siempre han planteado retos al derecho*" porque estos inciden, entre otros, "en el ejercicio de los derechos fundamentales de las personas" y por ende "*demandan diferentes respuestas del ordenamiento jurídico*".[28]

Según la Corte, internet es uno de esos avances "cuyos efectos a nivel transnacional plantea diversos problemas constitucionalmente relevantes"[29] porque, entre otras, se trata de una realidad importante en nuestra sociedad sobre la cual las herramientas jurídicas actuales pueden resultar insuficientes. En efecto, para dicha corporación "la existencia de una nueva red mundial de comunicaciones y de vías de circulación de información accesibles fácil y directamente al ciudadano para múltiples propósitos (…) a escala global *no es una realidad jurídicamente inocua*" y "la rapidez con la que evoluciona la tecnología que se emplea en internet, y al ingenio y creatividad de muchos de sus operadores, *los preceptos jurídicos expedidos con el propósito de regular las actividades que se desarrollan por este medio de comunicación pueden resultar inocuos para alcanzar algunas de las finalidades que persiguen*".[30] Por eso, concluye la Corte, en los caso casos que "la regulación existente resulte ineficaz para alcanzar los objetivos que orientan su creación, a causa de las novedades técnicas que se presentan" le corresponde a la rama legislativa "tomar las decisiones que cada evento amerite".[31]

A pesar que el campo de acción de internet desborda las fronteras nacionales, para la Corte el nuevo escenario tecnológico y las actividades en

[26] Todas las partes o frases señaladas entre comillas son tomadas de la sentencia C-1147 de 2001.

[27] Los otros derechos importantes que cita la Corte son: el derecho a la igualdad, la libertad de conciencia o de cultos, la libertad de expresión, el libre ejercicio de una profesión u oficio, el secreto profesional y el ejercicio de los derechos políticos que permiten a los particulares participar en las decisiones que los afectan (Corte Constitucional, C-1147 de 2001).

[28] Cursiva ausente en el original. Todas las partes o frases señaladas entre comillas son tomadas de la sentencia C-1147 de 2001.

[29] *Loc. cit.*

[30] Cursiva ausente en el original.

[31] *Loc. cit.*

internet no se sustraen del respeto de los mandatos constitucionales.[32] Por eso, concluye dicha entidad que "*en internet* (…) *puede haber una realidad virtual pero ello no significa que los derechos*, *en dicho contexto*, *también lo sean*. Por el contrario, no son virtuales: *se trata de garantías expresas por cuyo goce efectivo en el llamado 'ciberespacio'* también debe velar el juez constitucional".[33] Recalca dicha Corporación que "nadie podría sostener que, por tratarse de internet, los usuarios sí pueden sufrir mengua en sus derechos constitucionales".[34]

Visto lo anterior, en las siguientes líneas iniciaremos el estudio del derecho al olvido, planteando hipótesis ilustrativas de su aplicación.

II. El derecho al olvido como una acepción del derecho de supresión y una concreción del derecho de oposición: anotaciones sobre las primeras regulaciones latinoamericanas y europeas

Los fundamentos,[35] la definición y el alcance del derecho al olvido dependerá de lo que digan las regulaciones y de las interpretaciones jurisprudenciales o de las decisiones o pronunciamientos de las autoridades de cada país. A la fecha, encontramos que este derecho se incorporó expresamente y desde 2012 en países latinoamericanos (Nicaragua y Costa Rica) y posteriormente en Europa (2016). Estas referencias normativas son referentes iniciales del tema. Su análisis en cada país dependerá del marco jurídico del mismo. Por eso, no es recomendable generalizar el tema en términos abstractos, sino precisarlo a la luz de las regulaciones de cada Estado.

El artículo 10 de la Ley 787 de 2012[36] de la República de Nicaragua se titula "Derecho al olvido digital" y su contenido es el siguiente:

[32] En efecto, subraya la Corte Constitucional que "los mandatos expresados en la Carta Política cobran un significado sustancial que demanda del juez constitucional la protección de los derechos reconocidos a todas las personas, pues se trata de garantías que también resultan aplicables en ese ámbito" (Corte Constitucional, C-1147 de 2001)

[33] Cursiva ausente en el original.

[34] Todas las partes o frases señaladas entre comillas son tomadas de la sentencia C-1147 de 2001.

[35] Sobre los fundamentos del derecho al olvido consúltese, entre otros: Leturia, Francisco, "Fundamentos jurídicos del derecho al olvido. ¿un nuevo derecho de origen europeo o una respuesta típica ante colisiones entre ciertos fundamentos?", en: *Revista Chilena de Derecho de la Pontificia Universidad Católica de Chile*, Vol. 43, No.1, Santiago, Facultad de Derecho, abril, 2016. Disponible en: http://bit.ly/2flFo0Z.

[36] Ley de Protección de Datos Personales. Aprobada el 21 de marzo de 2012 y publicada en *La Gaceta*, No. 61, del 29 de marzo de 2012. Disponible en: http://bit.ly/2flybOn.

> El titular de los datos tiene derecho a solicitar a las redes sociales, navegadores y servidores que se supriman y cancelen los datos personales que se encuentren en sus ficheros.
> En los casos de ficheros de datos de instituciones públicas y privadas que ofrecen bienes y servicios y que por razones contractuales recopilan datos personales una vez terminada la relación contractual, el titular de los mismos puede solicitar que se suprima y cancele toda la información personal que se registró mientras era usuario de un servicio o comprador de un bien.

Como se observa, el derecho al olvido se trata como sinónimo del derecho de cancelación o supresión, que hacen parte de los derechos ARCO, a los que se refieren expresamente algunas regulaciones latinoamericanas como la mexicana.[37] Nótese cómo el primer párrafo no especifica los motivos o circunstancias en las cuales procede el derecho al olvido frente a las redes sociales, navegadores y servidores. Por eso, serán los mismos para solicitar la supresión o cancelación del dato. En el caso de la existencia de una relación contractual frente a instituciones públicas y privadas el derecho al olvido puede ejercitarse cuando la misma culmina.

El artículo 11 del Decreto 37.554 de 2012[38] de la República de Costa Rica bajo el título de "Derecho al olvido", establece lo siguiente: "La conservación de los datos personales, que puedan afectar a su titular, no deberá exceder el plazo de diez años, desde la ocurrencia de los hechos registrados, salvo disposición normativa especial que establezca otro plazo o porque el acuerdo de las partes haya establecido un plazo menor. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados los datos personales de su titular". Como se observa, el artículo vincula el derecho al olvido con la vigencia del dato personal cuya información lo pueda afectar. Para el efecto, establece un plazo objetivo predeterminado y general como punto de referencia.

El derecho al olvido también fue incluido en el artículo 17 del del

[37] *Cfr*. Remolina Angarita, Nelson, "Los derechos de acceso, rectificación, cancelación y oposición en la ley de datos personales y su reglamento", *La protección de datos personales en México*, México, D.F., Tirant Lo Blanch, 2013, pp. 181-205.

[38] Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales del 30 de octubre de 2012. El texto del decreto se puede consultar en: http://bit.ly/2gy3JFl.

Reglamento (UE) 2016/679[39] General de Protección de Datos Personales (RGPDP). Aunque se menciona como tal –"derecho al olvido"–, realmente no es un nuevo derecho autónomo e independiente, sino que se trata de una acepción del derecho de supresión, el cual ya existía en la Directiva 95/46/CE. No obstante, en el nuevo reglamento fueron ampliadas las hipótesis en que procede la supresión de los datos personales.

En efecto, de conformidad con el literal "b" del artículo 12 de la Directiva 95/46/CE, el titular del dato tenía derecho a solicitar al responsable del tratamiento "la supresión o el bloqueo de sus datos" cuyo tratamiento no se ajustará a lo ordenado por dicha directiva y especialmente cuando los datos fuesen incompletos o inexactos. Llama mucho la atención la expresión "bloqueo" porque ella puede referirse a la desindexación de información de manera que se impida el acceso a determinada información. Como consecuencia de la supresión, el titular también tiene derecho a que el responsable notifique a quienes le había comunicado la información objeto de supresión para que tuviesen conocimiento que la misma fue eliminada.

Ahora bien, si supresión es igual al "derecho al olvido", debemos anotar que este derecho no es novedoso en documentos internacionales sobre tratamiento de datos personales cuyas principales referencias destacamos en la siguiente tabla:

[39] *Cfr*. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

	Derecho de supresión o cancelación
Directrices OECD de 1980 y 2013	"Principio de participación individual. La persona debería tener derecho a: (…) d) impugnar los datos que se refieran a ella y, si la impugnación prospera, hacer que se supriman, rectifiquen, completen o modifiquen los mismos" (numeral 13).
Convenio 108 de 1981	"Artículo 8. Garantías complementarias para la persona concernida. Cualquier persona deberá poder: (…) c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio".
Resolución 45/95 de la ONU (1990)	"4. Principio de acceso de la persona interesada. Toda persona que demuestre su identidad tiene derecho a (…) obtener las rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, injustificados o inexactos".
Directiva 95/46/CE	"Artículo 12. Derecho de acceso. Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: (…) b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos; c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado".
Marco de Privacidad APEC (2004)	"VIII. Acceso y Corrección. 23. Los individuos deben ser capaces de: (…) c) desafiar la exactitud de la información relacionada con ellos y, si es posible y como sea adecuado, rectificar, completar, corregir o borrar la información".
Directrices de la Red Iberoamericana de Protección de Datos (2007)	"5. Derechos de acceso, rectificación y cancelación de los interesados. El interesado cuyos datos sean objeto de tratamiento podrá, a través de procedimientos claros, expeditos y gratuitos o sin gastos excesivos: (…) 5.3. Exigir, en su caso, la rectificación o cancelación de los datos que pudieran resultar incompletos, inexactos, inadecuados o excesivos, con arreglo a lo previsto en las presentes directrices. 5.4. Exigir que se notifique a los terceros a quienes se hayan comunicado los datos de toda rectificación o cancelación efectuado conforme al párrafo anterior".
Resolución de Madrid (2009)	"17 Derecho de Rectificación y cancelación 1. El interesado tendrá derecho a solicitar a la persona responsable la rectificación o cancelación de los datos de carácter personal que pudieran resultar incompletos, inexactos, innecesarios o excesivos. 2. Cuando proceda, la persona responsable rectificará o cancelará los datos de carácter personal conforme a lo solicitado. Deberá, además, notificar este extremo a los terceros a quienes se hayan comunicado los datos de carácter personal, siempre que los mismos fueran conocidos".

Tabla No. 1. El derecho de supresión o cancelación en documentos internacionales.

Fuente: Elaboración del autor40

Suprimir significa, entre otras, "hacer cesar, hacer desaparecer".[41] En otras palabras se refiere a eliminar, quitar, erradicar o destruir datos personales. La supresión se asimila a la cancelación de los derechos ARCO. En algunos documentos internacionales[42] la cancelación procede en situaciones donde está en duda la veracidad de los datos personales. Frente a dichas situaciones el titular puede optar por solicitar la rectificación o la cancelación (supresión). La primera supone que la información se corrija y se sigua tratando mientras la segunda tiene como finalidad culminar el tratamiento de los datos personales debido a la mala calidad de la información.

Creemos que el titular puede solicitar la eliminación o cancelación de sus datos cuando:

- El tratamiento de los datos es prohibido.
- Los datos se obtuvieron ilegítimamente.
- La información es falsa o no cumple los requisitos que demanda el principio de veracidad o calidad.
- Ha expirado el límite temporal del tratamiento de los datos personales (en los casos que exista dicho límite en la regulación).
- Los datos recolectados son inadecuados, innecesarios o excesivos respecto de la finalidad del tratamiento.
- Se ha cumplido la finalidad del tratamiento.
- Cuando en situaciones concretas y de manera injustificada se afectan derechos fundamentales de la persona. En este caso, proceden situaciones de informaciones verdaderas sobre el pasado de la persona que en contextos especiales y excepcionales ameritan que la información sea olvidada.

Esto último también se vincula, en algunos casos, al derecho de oposición que también ha sido objeto de mención en algunos documentos internacionalales tal y como lo evidenciamos a continuación:

[40] La cursiva nos pertenece.

[41] Definiciones tomadas del *Diccionario de la Real Academia Española*.

[42] *Cfr*. (i) Red Iberoamericana de Protección de Datos. Directrices para la armonización de la protección de datos en la comunidad Iberoamericana (2007), y (ii) Estándares Internacionales para la Protección de la Privacidad, en relación con el Tratamiento de Datos de Carácter Personal, acogida favorablemente por la 31º Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid.

	Cuando procede el derecho de oposición
Directiva 95/46/CE	Art. 14: Derecho a oponerse en cualquier momento y *por razones legítimas propias de su situación particular*, a que los datos que le conciernan sean objeto de tratamiento. También procede la oposición cuando se trate de un tratamiento destinado a la prospección.
Directrices de la Red Iberoamericana de Protección de Datos (2007)	Art. 6.2: En casos no excluidos en la ley en donde exista una "razón excepcional y legítima derivada de su concreta situación personal". Art. 6.3: Cuando los datos sean objeto de tratamiento para *"actividades vinculadas con la publicidad y la prospección comercial"*.
Resolución de Madrid (2009)	Art. 18: "cuando concurra una razón legítima derivada de su concreta situación personal".

Tabla No. 2 Casos en los que procede el derecho de oposición según documentos internacionales. Fuente: Elaboración de Nelson Remolina[43]

En síntesis, frente a la falta de definición universal del derecho al olvido, creemos que este no solo es el clásico derecho de eliminación de información, sino que guarda relación con el derecho de oposición que permite a las personas que en excepcionales circunstancias solicite la eliminación negativa y verdadera de su pasado.

Visto lo anterior, a continuación nos referiremos al artículo 17 del nuevo reglamento europeo de protección de datos personales.

II.A. Del artículo 17 del Reglamento (UE) 2016/679: derecho de supresión ("el derecho al olvido")

La regulación europea sobre el tratamiento de datos personales ha incidido en la normas de los países latinoamericanos a tal punto que en muchas cuestiones las leyes de los últimos países son iguales o similares a lo que establecen las disposiciones europeas. Adicionalmente, el nuevo Reglamento, por primera vez, se refiere expresamente sobre el derecho al olvido, lo cual nos ayudará a comprender de qué se trata. Todo lo anterior denota la importancia y relevancia de conocer el alcance de la reciente normativa europea.

Antes de referirnos al contenido del artículo 17, resulta pertinente señalar que el derecho al olvido supone, entre otros, una limitación temporal al tratamiento de los datos personales. La regla general consiste en que no

[43] La cursiva nos pertenece.

habrá tratamientos perennes de los datos. En ese sentido, el reglamento consagra el principio de "imitación del plazo de conservación" según el cual los datos serán utilizados "durante no más tiempo del necesario para los fines del tratamiento de los datos personales".[44]

El reglamento trata el derecho al olvido como sinónimo del derecho de supresión que existía previamente no solo en la Directiva 95/46/CE sino en otros documentos internacionales. Además de suprimir el dato, el responsable deberá adoptar medidas razonables para informar a quienes tratan los datos que son objeto de supresión con miras a que, asumimos, dejen de tratarlos.[45]

II.A.1. Casos en que proceden el derecho de supresión o "derecho al olvido"

Como regla general, el artículo 17[46] establece que el titular tiene el derecho

[44] *Cfr*. Literal "e" del artículo 5 del RGPDP.

[45] *Cfr*. Numeral 2 del artículo 17 del RGPDP. Sobre este aspecto, la exposición de motivos del Reglamento dice lo siguiente: "66. A fin de reforzar el 'derecho al olvido' en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales. (67) Entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema".

[46] La exposición de motivos del RGPDP dice lo siguiente: "65. Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un 'derecho al olvido' si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe

a solicitar la supresión de sus datos personales y el responsable del tratamiento, por su parte, debe proceder a eliminar "sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes":

los datos personales ya *no sean necesarios en relación con los fines* para los que fueron recogidos o tratados de otro modo.[47]

En este caso, será forzoso establecer cuándo los datos personales ya no son necesarios para el propósito que fueron recolectados. Piénsese, por ejemplo, cuando los datos son tratados para efectos de un proceso de selección de personal para suplir un cargo en una empresa. Una vez que culmine el proceso, se debería suprimir los datos de las hojas de vida de las personas que no fueron contratadas para trabajar con dicha corporación.

• *el interesado retire el consentimiento* en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), *y este no se base en otro fundamento jurídico.*[48]

El reglamento establece que, entre otras, el tratamiento es lícito si el titular del dato (o interesado) autorizó[49] la recolección y uso de su información para uno o varios fines específicos.[50] De igual forma, se requiere el consentimiento explícito del titular de datos especiales como los sensibles.[51] Si el titular revoca su consentimiento se debe suprimir los datos salvo que exista otro fundamento jurídico que impida dicha eliminación.

---

ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones".

[47] La cursiva nos pertenece.

[48] La cursiva nos pertenece.

[49] El consentimiento es definido como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen" (numeral 11 del artículo 4 del RGPDP).

[50] *Cfr*. Literal "a" del apartado 1 del artículo 6 del RGPDP.

[51] Se refiere a datos personales que "revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física" (numeral 1 del artículo 9 del RGPDP).

• *el interesado se oponga al tratamiento* con arreglo al artículo 21, apartado 1, *y no prevalezcan otros motivos legítimos para el tratamiento*, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2.[52]

Tal y como sucede en otros documentos internacionales, el RGPDP ratifica que en los casos de oposición al tratamiento es factible que se produzca la supresión de los datos. Según el artículo 21 del Reglamento, el titular de los datos tiene derecho a oponerse "en cualquier momento, *por motivos relacionados con su situación particular*, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones".[53] Como situaciones particulares, nos referimos, por ejemplo, a los casos enunciados en la parte 2 de este texto.

Cuando se presenten situaciones particulares, "*el responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado*, o para la formulación, el ejercicio o la defensa de reclamaciones".[54] Este será el factor determinante para decidir si en los casos del numeral 2 de este artículo procede o no a conceder el derecho al olvido o de supresión.

Finalmente, al igual que otros documentos internacionales, el derecho de oposición también procede cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa.

• los datos personales hayan sido *tratados ilícitamente*[55].

El tratamiento es ilícito cuando no se basa en algunos de los supuestos del artículo 6 del RGPDP.

• los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

• los datos personales se hayan obtenido *en relación con la oferta de servicios*

[52] La cursiva nos pertenece.
[53] La cursiva nos pertenece.
[54] *Íd*.
[55] *Íd*.

de la sociedad de la información mencionados en el artículo 8, apartado 1.[56]

El apartado 1 del artículo 8 se refiere a condiciones aplicables al consentimiento de niños menores de 6 años en relación con los servicios de la sociedad de la información.

II.A.2. Casos en los que no procede el derecho de supresión o "derecho al olvido"

El derecho al olvido no es absoluto. Su ejercicio no tiene cabida en una serie de casos que se enuncian en el numeral 3 del artículo 17 y que nos permitimos transcribir a continuación:

- para ejercer el derecho a la libertad de expresión e información.

Sobre este aspecto debe anotarse que en el capítulo IX del REPDP se fijaron reglas exclusivas para situaciones especiales de tratamiento. Dentro de dichos entornos específicos se encuentra la libertad de expresión y de información.

El artículo 85 del RGPDP ordena a los Estados establecer mediante ley pautas para conciliar "el derecho a la protección de los datos personales" con "el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria".

En particular, el artículo ordena crear las exenciones o excepciones que sean necesarias para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria con miras a conciliar los derechos citados, respecto de lo dispuesto en el REPDP sobre "lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos)".

Como se observa, el tema queda condicionado a la intervención del regulador de cada Estado miembro.

- para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de

[56] *Íd*.

una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

• por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

• con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

• para la formulación, el ejercicio o la defensa de reclamaciones.

Visto lo anterior, en las siguientes líneas nos referiremos al primer caso sobre el tema que encontramos en la jurisprudencia latinoamericana, el cual nos parece importante traer a colación con miras a destacar el principal fundamento de este derecho.

III. Del surgimiento jurisprudencial del derecho al olvido en Latinoamérica y su vinculación con la dignidad humana

El derecho al olvido surgió jurisprudencialmente en Colombia en 1992.[57] En aquel entonces, la Corte Constitucional revisó una acción de tutela de una persona que aparecía reportada como deudor moroso en una central de información financiera a pesar que habían transcurrido cuatro años desde la declaratoria judicial de la prescripción de la obligación dineraria. De entrada, la Corte se refirió, entre otras, a lo que en ese entonces denominó "la cárcel del alma y el derecho al olvido"[58] afirmando que "el encarcelamiento del alma en la sociedad contemporánea, dominada por la imagen, la información y el conocimiento, ha demostrado ser un mecanismo más expedito para el control social que el tradicional encarcelamiento del cuerpo". Así las cosas, desde hace veinticuatro años se anunciaban algunos efectos que

[57] Un análisis del caso colombiano junto con un análisis comparado sobre el derecho al olvido puede consultarse en: Manrique Gómez, Valentina, "El derecho al olvido: análisis comparativo de las fuentes internacionales con la regulación colombiana", en: *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, No. 14, Universidad de los Andes, diciembre, 2015. Disponible en: http://bit.ly/2f2QCMF.

[58] Corte Constitucional, sentencia T-414 del 16 de junio de 1992, MP, doctor Ciro Angarita Barón.

puede generar sobre los derechos de las personas la difusión perenne de información negativa sobre las mismas.

En sentencia T-414 del 16 de junio de 1992, la Corte Constitucional concluyó que se vulneró:

> La intimidad, la libertad personal y la dignidad del petente mediante el abuso de la tecnología informática y del derecho de y a la información. La vulneración de tales derechos constitucionales fundamentales se materializa en la renuencia de la Asociación Bancaria de Colombia a cancelar su nombre de la lista de deudores morosos y actualizar inmediatamente la información de su banco de datos computarizado, a sabiendas de que mediante sentencia del 27 de abril de 1987 debidamente ejecutoriada, un juez de la República declaró prescrita la obligación del señor (…) con el Banco de Bogotá.

Para la Corte, el derecho al olvido "le fue abiertamente negado al peticionario" al condenarlo "sin fórmula de juicio, a una exclusión del sistema crediticio por término indefinido". Por eso, la Corte ordenó "la inmediata cancelación del nombre del peticionario (…) de la lista de deudores morosos de la Central de Información".

Resulta de enorme importancia destacar lo siguiente que estableció la Corte en la citada sentencia:

- El tratamiento de los datos personales "tiene una vigencia limitada en el tiempo".
- Las "sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia después de algún tiempo tales personas son titulares de un verdadero derecho al olvido".
- "Con la consagración expresa que se ha hecho de la dignidad humana como el valor supremo del Estado Social de Derecho, (artículo 1º de la Carta de 1991), la intimidad, que es una de las manifestaciones más concretas y directas de dicha dignidad, ha adquirido una posición privilegiada en el conjunto de los derechos constitucionales fundamentales. Esto implica, se reitera una vez más, que *ante un eventual conflicto insuperable entre el derecho a la información y el derecho a la intimidad en donde no pueda ser posible un equilibrio o coexistencia, la intimidad deberá prevalecer*".[59]
  En posteriores decisiones, la Corte destacó la conexidad entre el derecho

[59] La cursiva nos pertenece.

al olvido y la dignidad humana, recalcando que la información, así sea verdadera, no debe publicarse eternamente cuando ello afecta la dignidad de la persona. Así por ejemplo, mediante la sentencia T-022 de 1993, esa corporación manifestó que:

> La verdad no es, pues, la llave milagrosa que abre dicho muro –intimidad– y expone al sujeto a observación inclemente, como pez en acuario de cristal. No. La verdad cede aquí el paso a la dignidad de la persona y a los riesgos previsibles de la autodeterminación y la maduración en el ejercicio de la libertad. Como lo ha venido señalando la más autorizada doctrina jurídica y las corrientes filosóficas que hacen de la persona su eje vital, no es procedente, por razones apenas obvias, la socorrida exceptio veritatis.[60]

En la sentencia T-592 de 2003, por su parte, la Corte concluyó que:

> El derecho al olvido, a fin de restablecer el buen nombre, no es lo único que cuenta en la definición de los límites de permanencia de los datos adversos en los ficheros de datos, también la dignidad del deudor reclama que la valoración de su conducta se realice en consideración a su condición humana, en función de la cual las personas pueden en todo tiempo recuperar su nombre e intimidad por haber enmendado su conducta.[61]

De lo anterior, consideramos que surgieron los siguientes parámetros para considerar en casos futuros que involucren situaciones del derecho al olvido:

- Por regla general, no deberían existir tratamientos perpetuos de los datos

[60] Subrayado original del texto de la sentencia. *Cfr*. Corte Constitucional, sentencia T-022 del 21 de enero de 1993, MP, doctor Ciro Angarita Barón. En dicha sentencia, remató sus argumentos la Corte con lo siguiente: "Esta corporación cree oportuno advertir también que el derecho a la intimidad no se construye en todos los casos con materiales extraídos de las canteras de la verdad o bondad absolutas, sino con los más humildes y propios de la conducta humana en todas sus complejas manifestaciones. Por tanto, ni la exceptio veritatis, ni la presunta o real existencia de una conducta desviada son consideraciones suficientes para desconocer el derecho a la intimidad, con todos los alcances establecidos por el Constituyente en el artículo 15 de la Carta. Bondad, probidad e intimidad operan, pues, en órbitas no necesariamente coincidentes o iguales" (subrayado del original).

[61] Corte Constitucional, sentencia T-592 del 17 de julio de 2003, MP, doctor Álvaro Tafur Galvis.

personales.
- Así sean ciertos los datos que se tratan sobre una persona, no se le puede condenar a que su información negativa sea conocida indefinidamente por todos.
- Ni la intimidad ni el derecho a la información son absolutos. Ambos son importantes en una sociedad democrática. No obstante, la dignidad humana es un factor determinante para tomar decisiones frente a situaciones concretas que se debatan ante los jueces. No es sensato inclinarse, per se, hacia uno o hacia otro derecho, porque las particularidades de cada caso ameritan un análisis especial.

En suma, desde 1992 surgió en Colombia una doctrina constitucional sobre el derecho al olvido. Lo importante de la misma es reconocer que la información negativa, así sea verdadera, no siempre debe publicarse de manera ilimitada y eterna. Existen casos en los que es necesario limitar dicha publicación por cuestiones de dignidad humana u otras razones que pueden derivarse de casos concretos.

Conclusiones

El derecho al olvido ha cobrado especial relevancia frente a publicaciones en internet de hechos verdaderos del pasado de las personas, que ahora, por motivos particulares de los afectados, desean que se suprima definitivamente. Al mismo tiempo, el ciberespacio es el contexto en donde principalmente tienen lugar dichas situaciones, lo cual hace muy difícil lograr que se materialice efectivamente el derecho al olvido en dicho escenario digital, transfronterizo e incontrolable tanto por la cantidad de cibernautas, como por el diseño de red global, abierta y de fácil acceso que tiene internet.

El 16 de junio de 1992 nació expresamente en Colombia el derecho al olvido como fruto de la labor de la Corte Constitucional. Con ese derecho se busca que en situaciones concretas y legítimas se deje de publicar o difundir información negativa y verdadera del pasado de las personas. En ciertos casos no es sensato publicar de manera ilimitada y eterna la información negativa ya que es imperioso limitar dicha publicación por cuestiones de dignidad humana u otras razones que pueden derivarse de casos concretos. Por eso, en cada situación particular será necesario establecer si frente a la situación de la persona que se opone al tratamiento de sus datos del pasado, prevalecen otros motivos legítimos para continuar tratando dicha información.

El derecho al olvido es importante para las personas que quieren cambiar su vida respecto de lo que han hecho en el pasado: ¿Tiene derecho una trabajadora sexual a cambiar de oficio, replantear su vida, casarse, tener hijos, estudiar y vivir el presente y el futuro sin que la gente conozca su pasado? ¿Debe condenarse eternamente a las personas por su pasado? ¿Tienen derecho las personas a tomar la decisión de optar por otra forma de vivir sin que los persiga el fantasma negativo de su pasado? Si la respuesta es afirmativa, ¿cómo hará esa persona para cambiar si vía internet, las noticias, videos o en el cine se difunde el pasado negativo de ella? Las respuestas, desde luego, variarán caso por caso pero es importante determinar, entre otras, si el pasado negativo de una persona es de interés público y socialmente relevante como para que se continúe difundiendo en el presente y en el futuro.

Para muchas personas es transcendental el reconocimiento y la garantía del derecho al olvido. Ese puede ser, quizás, el único camino con que cuenten para que no las sigan estigmatizando o condenando perpetuamente por hechos ciertos y negativos de su pasado.

Las primeras regulaciones que expresamente se refieren al derecho al olvido son latinoamericanas (Nicaragua y Costa Rica en 2012) y posteriormente europeas (2016). En las primeras, el derecho al olvido está asociado a la vigencia temporal de la información y a la supresión o cancelación de la misma.

Frente a la reciente reglamentación europea sobre el derecho al olvido persisten vacíos sobre su definición porque consideramos que este no solo es el clásico derecho de supresión de información, sino que guarda relación con el derecho de oposición que permite a las personas que en excepcionales circunstancias soliciten la eliminación negativa y verdadera de su pasado. Adicionalmente, el transcurso del tiempo es un factor adicional e importante para establecer que estamos frente a dicho derecho porque los casos jurisprudenciales normalmente tratan información negativa y verdadera del pasado de las personas.

El derecho al olvido no es absoluto. Su protección dependerá del analisis de las diversas variables que surjan de las pecularidades de casos concretos y reales. No obstante, no debe olvidarse que las personas tienen derecho a modificar su vida sin que las persiga permanente e indefinidament el fantasma negativo de su pasado.

Los motores de búsqueda no son quienes generan la información, pero sí son los principales responsables de difundir masiva e instantáneamente la información que existe en internet. Ignorar los efectos multiplicadores y globales de los motores de búsqueda y de la indexación es como desconocer que existe internet.

No se puede perder de vista que la indexación por parte del motor de búsqueda es lo que facilita que la información se conozca fácilmente en

internet. El motor de búsqueda colabora en la difusión de la información desactualizada sobre una persona. La indexación es el detonante de la multiplicación ilimitada de los datos personales en la red. Llama mucho la atención que algunos asuman ciega y acríticamente que indexar información es "normal", pero desindexarla para proteger derechos humanos o la dignidad humana es "terrible" o "muy grave".

Finalmente, terminamos este texto con la frase que iniciamos el mismo: ¿Tienen derecho las personas a cambiar su vida, sin que las persiga eternamente el fantasma de la información negativa de su pasado que ha sido difundida en internet? Si su respuesta es positiva, entonces ha comprendido la importancia del derecho al olvido.

Hacia una Internet libre de censura II

Perspectivas en América Latina

El Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) fue creado en el año 2009 en el ámbito de la Facultad de Derecho de la Universidad de Palermo con el objetivo de proveer de investigaciones a periodistas, instituciones gubernamentales, unidades académicas, sectores privados y de la sociedad civil dedicados a la defensa y a la promoción de estos derechos, especialmente en América Latina.

La creación del CELE responde a la necesidad de construir espacios de debate dedicados a reflexionar sobre la importancia, los contenidos y los límites de la libertad de expresión y el acceso a la información en la región. Para esto, el centro se propone dialogar y trabajar en conjunto con otras unidades académicas del país y de Latinoamérica.

En este marco, los objetivos específicos del CELE son:

- Desarrollar estudios y guías de recomendaciones que tengan impacto en las políticas públicas vinculadas con el acceso a la información y a la libertad de expresión.
- Fomentar junto con distintas unidades académicas la profundización de estudios en cuestiones vinculadas con estos derechos.
- Contribuir a la generación de conciencia sobre la importancia de estos derechos en sociedades democráticas, fundamentalmente en las nuevas generaciones.

Este libro fue realizado en el marco de un proyecto auspiciado por Ford Foundation.

UP Universidad de Palermo

CELE

ISBN 978-950-9887-20-6

9 789509 887206

Facultad de Derecho
Centro de Estudios en Libertad de Expresión y Acceso a la Información
Mario Bravo 1050, 7° P. (C1175ABT) Buenos Aires | Tel.: (54 11) 5199-4500 int. 1213
www.palermo.edu/cele