Introducción a la

GOBERNANZA DE INTERNET

Jovan Kurbalija

7ª Edición

DiPLO
www.diplomacy.edu

La historia de este libro es extensa en el tiempo de vida de Internet. El texto original y el enfoque general, incluida la metodología de las cinco canastas, se desarrollaron en 1997 para un curso de capacitación sobre políticas de tecnologías de la información y comunicación (TIC) para funcionarios de gobierno de los países que conforman el Commonwealth. En 2004, Diplo publicó una versión impresa de nuestros materiales sobre gobernanza de Internet, en un cuadernillo intitulado Internet Governance – Issues, Actors and Divides. Este libro formó parte de la Biblioteca de la Sociedad de la Información, una iniciativa de Diplo impulsada por Stefano Baldi, Eduardo Gelbstein, y Jovan Kurbalija. En 2008 se publicó una versión especial y revisada del libro, que llevó el simple título de *An Introduction to Internet Governance*, en colaboración con NIXI India durante la celebración del Foro de Gobernanza de Internet (IGF, por sus siglas en inglés) en Hyderabad, India. En 2009 se dio a conocer una tercera edición, revisada, en cooperación con el Ministerio de Tecnología de Información y Comunicación de la Gobernanza de Internet de Egipto. La cuarta edición (2010) se elaboró en sociedad con la Secretaría de los Estados de África, el Caribe y el Pacífico, y la Unión Europea. La quinta edición (2012) se publicó en colaboración con la Academia Diplomática de Azerbaiyán (ADA). En septiembre de 2014 se publicó la sexta edición. El difunto Eduardo Gelbstein realizó importantes contribuciones a las secciones que abordan la ciberseguridad, el correo no deseado, y la privacidad.

Queremos agradecer al equipo de curadores que está trabajando en el observatorio GIP Digital Watch, quienes realizaron aportes a la actualización de varias partes de la edición 2016: Radek Bejdak, Stephanie Borg Psaila, Katharina Höne, Tereza Horejsova, Arvin Kamberi, Aida Mahmutović, Adriana Minović, Virginia Paque, Roxana Radu, Vladimir Radunović, Barbara Rosen Jacobson, y Sorina Teleanu. Stefano Baldi, Eduardo Gelbstein, y Vladimir Radunović contribuyeron enormemente al desarrollo de los conceptos detrás de las ilustraciones del libro. Reconocemos los comentarios y sugerencias de otros colegas en el texto.

Introducción a la

GOBERNANZA DE INTERNET

Jovan Kurbalija

7ª EDICIÓN

DiPLO
www.diplomacy.edu

Publicado por DiploFoundation (2016)

Malta: DiploFoundation
Anutruf, Planta Baja
Calle Hriereb
Msida, MSD 1675, Malta

Suiza: DiploFoundation
7bis, Avenue de la Paix
CH 1211 Ginebra, Suiza

Serbia: DiploCentar
Braničevska 12a/12
11000 Belgrado, Serbia

Correo electrónico: diplo@diplomacy.edu
Sitio web: http://www.diplomacy.edu

Diseño y presentación: Viktor Mijatović
Tradución: Justina Díaz Cornejo
Edición (Español): María Eugenia Disandro
Ilustraciones: Dr. Vladimir Veljašević
Preimpresión e impresión: Aleksandar Nedeljkov

A menos que se especifique lo contrario, este trabajo está licenciado por **https://creativecommons.org/licenses/by/3.0/**

Se fomenta la traducción y la publicación de este libro en otros idiomas.
Para obtener más información, por favor contáctese con **diplo@diplomacy.edu**

Cualquier referencia que se presenta en este libro acerca de un producto en particular sirve meramente como modo de ejemplo y no debe considerarse como apoyo o recomendación del producto en sí.

Los iconos azules y los enlaces al final de varias subsecciones del libro indican que hay más material de fondo (desarrollos en curso, actores, eventos, instrumentos y recursos) disponibles en línea, en el observatorio *GIP Digital Watch*.

ISBN: 978-99932-53-31-0

DiPLO
www.diplomacy.edu

MÉXICO
GOBIERNO DE LA REPÚBLICA

ICANN

LACTLD
Latin American and Caribbean ccTLDs Organization

Contents

Prólogo

En 2004, cuando les comenté a mis amigos lo que estaba haciendo como miembro del GTGI – Grupo de Trabajo sobre Gobernanza de Internet – casi siempre me llamaban a mí para que arreglara sus impresoras o para que instalara un nuevo software en sus computadoras. Hasta donde ellos sabían, yo hacía algo relacionado con las computadoras. Recuerdo haberles hecho una breve encuesta a los otros miembros del GTGI en la que les preguntaba cómo les explicaban a sus amigos, parejas, e hijos a qué se dedicaban. Al igual que a mí, les resultaba difícil. Esta es una de las razones por las que comencé a diseñar y preparar el primer texto y dibujos de Diplo sobre la gobernanza de Internet.

Hoy, solo doce años después, esas mismas personas que me pedían que instalara sus impresoras me vuelven con preguntas sobre cómo mantener la posesión de sus datos en Facebook o sobre cómo asegurarse de que sus hijos puedan navegar en Internet de manera segura. Están cada vez más preocupados por una posible ciberguerra y por los riesgos en línea para los suministros de agua, las centrales eléctricas, y otros tipos de infraestructura crítica en sus países y ciudades. ¡A qué punto hemos llegado!

La gobernanza de Internet se posiciona cada vez más en el centro de la opinión pública. Mientras más fuerte sea la dependencia de la sociedad moderna con Internet, más relevante resultará la gobernanza de Internet. Lejos de ser territorio de unos pocos selectos, la gobernanza de Internet nos involucra a todos en mayor o menor medida, independientemente de que seamos uno de los 3,6 mil millones de usuarios de Internet o alguien que, sin ser usuario, dependa de las facilidades que provee.

Claramente, la gobernanza de Internet es más importante para aquellos que están integrados profundamente en el mundo electrónico, ya sea a través de los negocios electrónicos o de la red de contactos en Facebook. Aun así, posee un amplio alcance. Los funcionarios de gobierno, el personal militar, los abogados, los diplomáticos, y otros individuos que ofrecen bienes públicos o se encargan de preservar la estabilidad pública también entran dentro de los interesados. La gobernanza de Internet, y particularmente la protección de la privacidad y los derechos humanos, es un punto central para los activistas de la sociedad civil y para las organizaciones no gubernamentales. Para los innovadores alrededor del mundo, la gobernanza de Internet debe asegurar que la Internet se mantenga abierta para su desarrollo e innovación. Los inventores creativos de los futuros Google, Skype, Facebook, y Twitter están ahora mismo, en algún lugar, navegando por Internet. Actualmente se discute apasionadamente en debates sobre la neutralidad en la red. También, en foros sobre propiedad intelectual se debate si se beneficiarán a partir de la igualdad de oportunidades para el desarrollo de maneras nuevas y más creativas de usar Internet. Ya no resulta sencillo separar algunos de estos debates de sus múltiples repercusiones en los diversos sectores y partes interesadas.

Anhelo que este libro brinde una introducción clara y accesible a la gobernanza de Internet. Para algunos de ustedes, este será su primer contacto con el tema. Para otros, servirá de recordatorio de que, lo que están haciendo en sus áreas de especialización – ya sea en salud, comercio, gobierno o cualquier otra área electrónica – es parte de una familia más amplia de cuestiones de gobernanza de Internet.

El objetivo subyacente de un enfoque tan diverso es la modesta contribución a la preservación de Internet como un gran habilitador para miles de millones de personas en el mundo. Como mínimo, espero que abra su apetito y que los motive a adentrarse en este

asunto tan extraordinario y fluido. Manténganse actualizados. Sigan los desarrollos en http://www.diplomacy.edu/capacity/IG y http://www.diplomacy.edu/ig

Jovan Kurbalija
Director de DiploFoundation
Jefe de la Plataforma de Internet de Ginebra
Noviembre de 2016

Sección 1

INTRODUCCIÓN

Aunque la gobernanza de Internet se trata del núcleo del mundo digital, la gobernanza no puede ser manejada con una lógica digital-binaria de verdadero/falso y bueno/malo. En cambio, la gobernanza de Internet exige muchas sutilezas y matices de significado y percepción; por lo tanto, requiere un enfoque analógico, cubriendo un continuo de opciones, compensaciones, y compromisos.

Por consiguiente, este libro no intenta proporcionar declaraciones definitivas sobre cuestiones de gobernanza de Internet. Más bien, su objetivo es proponer un marco práctico para el análisis, la discusión, y la resolución de cuestiones significativas en el campo.

Introducción

La controversia que rodea a la gobernanza de Internet comienza en su definición. No es mera pedantería lingüística. La manera en la que se define a Internet refleja diferentes perspectivas, enfoques, e intereses políticos. Por lo general, los especialistas en telecomunicaciones observan a la gobernanza de Internet a través del prisma del desarrollo de una infraestructura técnica. Los especialistas en computación se interesan por el desarrollo de diferentes estándares y aplicaciones, como XML (eXtensible Markup Language) o Java. Los especialistas en comunicación hacen hincapié en la simplificación de la comunicación. Los activistas de derechos humanos ven a la gobernanza de Internet desde la perspectiva de la libertad de expresión, la privacidad, y otros derechos humanos fundamentales. Los abogados se enfocan en la jurisdicción y la solución de conflictos. Los políticos alrededor del mundo se concentran, principalmente, en las cuestiones que resuenan en sus electorados, como el tecno-optimismo (más computadoras = más educación) y las amenazas (ciberseguridad, cibercrimen, y protección de menores). Los diplomáticos se preocupan fundamentalmente por el proceso y la protección de los intereses nacionales. Esta lista de perspectivas profesionales potencialmente contrapuestas sobre la gobernanza de Internet no termina aquí.

Qué significa la gobernanza de Internet

La Cumbre Mundial sobre la Sociedad de la Información (CMSI)[1] elaboró la siguiente definición práctica de gobernanza de Internet:

> *La gobernanza de Internet es el desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivos roles, de principios, normas, reglas, procedimientos de toma de decisiones, y programas comunes que dan forma a la evolución y a la utilización de Internet.*[2]

Esta definición práctica y un tanto amplia no soluciona la cuestión de las diferentes interpretaciones en dos términos clave: «Internet» y «gobernanza».

Internet

El término «Internet» no cubre todos los aspectos existentes en los desarrollos digitales globales. Usualmente, otros dos términos – sociedad de la información y tecnología de la información y la comunicación (TIC) – se plantean de una manera más integral. Incluyen áreas que se encuentran más allá del dominio de Internet, como la telefonía móvil. Sin embargo, el argumento para el empleo del término «Internet» se ve reforzado por la rápida transición de la comunicación global hacia el uso del protocolo de Internet (IP) como el principal estándar técnico de las comunicaciones. La Internet, que ya es ubicua, continúa expandiéndose a un ritmo acelerado, no solo con respecto a la cantidad de usuarios sino también a los servicios que ofrece; los denominados servicios sobre la capa (*over-the-top*), como la voz sobre protocolo de Internet (VoIP, por sus siglas en inglés) o la televisión por protocolo de

Internet (IPTV), están cada vez más propagados, y son considerados crecientemente como los competidores de los servicios convencionales, como el de telefonía y televisión.

"I"nternet o "i"nternet y la señalización diplomática

Allá por 2003, la revista *The Economist* comenzó a escribir la palabra «Internet» con «i» minúscula. Otras revistas tomaron la misma postura luego de esto, como la *Associated Press* y *The New York Times*. Este cambio en la política editorial se inspiró en el hecho de que la Internet se había convertido en un elemento tan cotidiano, que había dejado de ser lo suficientemente único y especial como para merecer una letra inicial en mayúscula. La palabra «Internet» siguió el destino lingüístico de (t)elégrafo, (t)eléfono, (r)adio, y (t)elevisión, y otras invenciones del estilo.

La dicotomía entre escribir «Internet» o «internet» con una «i» mayúscula o minúscula fue tema de debate en la Conferencia de la Unión Internacional de Telecomunicaciones (UIT) en Antalya (noviembre de 2006), en donde se introdujo una dimensión política cuando apareció el término «Internet» en la resolución de la UIT sobre la gobernanza de Internet escrito con «i» minúscula en lugar de la más usual «I» mayúscula. David Gross, embajador de EE. UU. y coordinador de política internacional de Comunicaciones e Información, expresó su preocupación acerca de que el uso de la minúscula por parte de la UIT pudiera sugerir una intención de tratar a la Internet como a otros sistemas de telecomunicaciones internacionalmente gobernados por la UIT. Algunos interpretaron este hecho como una señal diplomática de la intención de la UIT para desempeñar un rol de mayor prominencia en la gobernanza de Internet.[3]

Gobernanza

En el debate sobre gobernanza de Internet, surgió la controversia por el término «gobernanza» y sus varias interpretaciones. Según una de ellas, la gobernanza es sinónimo de gobierno. En las primeras etapas del proceso de la CMSI, muchas delegaciones nacionales tenían este acuerdo inicial, lo que resultó en la interpretación basada en que la gobernanza de Internet debía ser asunto de los gobiernos y, consecuentemente, abordada a nivel intergubernamental con la participación limitada de otros actores, principalmente no estatales.

Existe una mayor confusión cuando nos referimos a cómo se usa el término «gobernanza» en algunas organizaciones internacionales. Un ejemplo es el del término «buena gobernanza», que ha sido utilizado por el Banco Mundial para promover la reforma de los estados, incrementando la transparencia, reduciendo la corrupción, y aumentando la eficiencia de la administración. En este contexto, el término «gobernanza» está directamente ligado a las funciones centrales del gobierno.

Estas interpretaciones entran en conflicto con un significado más amplio del término «gobernanza», que incluye la gobernanza de los asuntos de cualquier institución, incluidas las no gubernamentales. Este fue el significado que aceptó la comunidad de Internet, debido a que describe la manera en la que la Internet se ha gobernado desde sus comienzos.

La confusión terminológica se complica aún más con la traducción del término (*governance*, en inglés) a otros idiomas. En español, el término se refiere principalmente a las actividades públicas o al gobierno (gestión pública, gestión del sector público, y función de gobierno). La referencia a las actividades públicas o al gobierno también aparece en francés

(*gestion des affaires publiques, efficacité de l'administration, qualité de l'administration,* y *mode de gouvernement*). El portugués sigue un patrón similar cuando nos referimos al sector público y al gobierno (*gestão* pública y *administração* pública).

La evolución de la gobernanza de Internet

Etapas tempranas de la gobernanza de Internet (década de 1970–1994)

Internet comenzó como un proyecto gubernamental. A fines de la década de los sesenta, el gobierno de los Estados Unidos patrocinó el desarrollo de la Red de la Agencia de Proyectos de Investigación Avanzada (ARPANet), una red destinada a facilitar el intercambio de recursos digitales entre computadoras. A mediados de los setenta, con la invención del TCP/IP (Protocolo para el Control de Transporte/Protocolo de Internet), esta red evolucionó a la Internet que hoy conocemos.

Uno de los principios clave de la Internet es su naturaleza de distribución: los paquetes de datos pueden tomar caminos diferentes a través de la red, evitando las barreras tradicionales y los mecanismos de control. Este principio tecnológico se correspondió con un enfoque similar a la regulación de Internet durante sus primeras etapas. La Fuerza de Tareas de Ingeniería de Internet (IETF, por sus siglas en inglés), establecida en 1986, logró avanzar con el desarrollo de Internet mediante un proceso cooperativo, consensuado, y de toma de decisiones, que involucraba a una amplia variedad de individuos. No existía un gobierno central, ni tampoco una planificación central o un gran diseño.

Esto llevo al pensamiento de que la Internet era, de alguna manera, única y que proveería una alternativa a las políticas del mundo moderno. En su famosa obra llamada Declaración de independencia del ciberespacio, John Perry Barlow, el estadounidense ciberliberal y activista político, señala:

> *[La Internet] es inherentemente extranacional, inherentemente antisoberana y su soberanía [la de los estados] no puede aplicarse a nosotros. Nosotros mismos debemos resolver las cosas.*[4]

La guerra del DNS (1994–1998)

Este enfoque descentralizado sobre la gobernanza de Internet pronto comenzó a cambiar, debido a que los gobiernos y el sector de los negocios comprendieron la importancia de la red global. En 1994, la Fundación Nacional de las Ciencias de los Estados Unidos, que gestionaba la infraestructura crítica de Internet, decidió subcontratar el manejo del Sistema de Nombres de Dominio (DNS, por sus siglas en inglés) a una compañía estadounidense privada llamada Network Solutions Inc. (NSI). Esta movida no fue bien recibida por la comunidad de Internet, y resultó en la denominada «guerra del DNS».

Esta guerra incluyó a nuevos jugadores: organizaciones internacionales y estados nacionales. Llegó a su fin en 1998 con el establecimiento de una nueva organización: la Corporación para la Asignación de Nombres y Números en Internet (ICANN, por sus siglas en inglés), que se convirtió en la coordinadora de los principales recursos técnicos de Internet, a raíz de un contrato con el gobierno de los Estados Unidos. La ICANN se convirtió, posteriormente, en el foco de muchos de los debates sobre la gobernanza de Internet.

La Cumbre Mundial de la Sociedad de la Información (2003–2005)

La CMSI, celebrada en Ginebra (2003) y en Túnez (2005), ubicó de manera oficial el tema de la gobernanza de Internet en las agendas diplomáticas. El tema central de la fase de la Cumbre de Ginebra, precedida por una serie de comités preparatorios (*PrepComs*) y reuniones regionales, fue más bien amplio, con una variedad de temas relacionados con las TIC que presentaron los participantes. De hecho, durante las primeras reuniones preparatorias y regionales, no se utilizó el término «gobernanza de Internet».[5] El tema de la gobernanza de Internet se introdujo al proceso de la CMSI durante la reunión regional de Asia occidental en febrero de 2003; luego de la cumbre en Ginebra, se convirtió en un tema clave en las negociaciones de la CMSI.

Tras negociaciones prolongadas y arreglos de último momento, la CMSI de Ginebra en 2003 acordó establecer un Grupo de Trabajo sobre Gobernanza de Internet (GTGI), que preparó el informe[6] utilizado como la base para las negociaciones en la segunda cumbre CMSI, que se celebró en Túnez (noviembre de 2005). La Agenda de la CMSI de Túnez para la Sociedad de la Información ahondó en el tema de la gobernanza de Internet, incluso con la adopción de la definición propuesta por la CMSI, una lista de cuestiones de gobernanza de Internet, y el establecimiento del Foro de Gobernanza de Internet (IGF, por sus siglas en inglés), un cuerpo conformado por múltiples partes interesadas convocadas por la Secretaría General de la ONU para que funcione como un espacio para debatir temas de políticas públicas relativas a los elementos clave de la gobernanza de Internet.[7]

Desarrollos en 2006

Tras la cumbre de Túnez, tres desarrollos y eventos principales marcaron el debate de la gobernanza de Internet en 2006. El primero tuvo que ver con la expiración del memorándum de entendimiento (MoU, por sus siglas en inglés) y el establecimiento de uno nuevo entre ICANN y el Departamento de Comercio de los Estados Unidos. Algunos tenían la esperanza de que este evento cambiara la relación entre ICANN y el gobierno de EE. UU., y esperaban que lase convirtiera en un nuevo tipo de organización internacional. Sin embargo, mientras que el nuevo MoU debilitó el cordón umbilical entre ICANN y el gobierno de EE. UU., mantuvo a la vez la posibilidad de una eventual internacionalización del estado de ICANN.

El segundo evento de 2006 fue el IGF en Atenas. Fue el primero de ese tipo y, en muchos aspectos, sirvió de experimento en la diplomacia multilateral. Fue verdaderamente una reunión con múltiples partes interesadas. Todas las partes – estados, empresas, la comunidad académica y la técnica, junto con la sociedad civil – participaron en igualdad de condiciones. Además, contó con una estructura organizacional interesante para los eventos más importantes y los talleres. Los periodistas moderaron los debates y fue por eso por lo que el IGF se diferenció del típico formato de reuniones de la ONU. No obstante, algunos críticos alegaron que el IGF fue solamente un programa de entrevistas, sin ningún resultado tangible que diera como producto un documento final o un plan de acción.

El tercer desarrollo importante en 2006 fue el de la Conferencia de Plenipotenciarios de la UIT en Antalya, Turquía, en noviembre. Se eligió al nuevo Secretario General de la UIT: el Dr. Hamadoun Touré. El Secretario anunció que se concentrarían más en la ciberseguridad y en la asistencia para el desarrollo. También se esperaba que introdujera nuevas modalidades al enfoque de la UIT con respecto a la gobernanza de Internet.

Desarrollos en 2007

En 2007, el debate de ICANN se enfocó en el dominio .xxx (contenido para adultos), lo que reabrió los debates sobre numerosas cuestiones de gobernanza, incluido el cuestionamiento sobre si ICANN debería lidiar solamente con problemas técnicos o también con asuntos importantes para las políticas públicas.[8] Las intervenciones por parte de los Estados Unidos y otros gobiernos en este contexto plantearon más profundamente la pregunta de cómo los gobiernos nacionales deberían involucrarse en las deliberaciones de ICANN.

En el segundo IGF, que se mantuvo en noviembre en Río de Janeiro, el principal desarrollo fue añadir los recursos críticos de Internet (CIR, por sus siglas en inglés) (nombres y números) en la agenda.

Desarrollos en 2008

El mayor desarrollo de 2008, que continuará influenciando a la gobernanza de Internet y también a otras esferas políticas, fue la elección de Barack Obama como presidente de los Estados Unidos. Durante la campaña presidencial, Obama utilizó las herramientas de Internet y la Web 2.0 de manera intensiva. Algunos argumentan que esta fue una de las razones de su éxito. Su grupo de consejeros estaba compuesto por muchas personas de la industria de la Internet, incluido el CEO de Google. Además de su conciencia tecnológica, el presidente Obama apoyó el multilateralismo, que inevitablemente influyó en los debates de la internacionalización de ICANN y del desarrollo de un régimen de gobernanza de Internet.

En 2008, la neutralidad de la red[9] emergió como uno de los asuntos más importantes en la gobernanza de Internet. Este tema se discutió principalmente en EE. UU., entre dos bloques principales opuestos. Incluso figuró en la campaña presidencial de EE. UU., apoyada por Obama. La neutralidad de la red encuentra apoyo en la denominada industria de Internet, incluidas las compañías como Google, Yahoo!, y Facebook. Un cambio en la arquitectura de la Internet impulsado por una vulneración en la neutralidad de la red podría poner en peligro sus negocios. Por otro lado, se encuentran las compañías de telecomunicaciones, como Verizon y AT&T, los proveedores de servicios de Internet (PSI), y la industria de los servicios multimedia. Por diversas razones, estas industrias querrían ver algún tipo de distinción entre los paquetes que viajan a través de Internet.

Consulte la Sección 2 para conocer más acerca del debate sobre la neutralidad de la red.

Otro desarrollo relevante fue el rápido crecimiento de Facebook y de las redes sociales. Cuando se trata de gobernanza de Internet, el creciente uso de las herramientas de la Web 2.0 abrió el debate sobre la privacidad y la protección de datos en las plataformas de redes sociales.

Desarrollos en 2009

La primera parte de 2009 presenció el intento del *Washington Belt* de descifrar las implicaciones y futuras direcciones de las políticas de Obama relacionadas con Internet. Los

nombramientos de Obama para los puestos clave relacionados con Internet no representaron ninguna sorpresa. Fueron coherentes con el apoyo de Obama a una Internet abierta. Su equipo también impulsó la implementación del principio de la neutralidad de la red de acuerdo con las promesas que se hicieron durante su campaña.

Lo destacado del 2009 fue la conclusión de la *Afirmación de Compromisos* entre ICANN y el Departamento de Comercio de EE. UU., que tenía como propósito hacer de ICANN una organización más independiente. Mientras que esto representó un paso hacia adelante en el abordaje de un problema en la gobernanza de Internet – el rol de supervisión de EE. UU. sobre ICANN – ,muchas problemáticas nuevas emergieron, como la posición internacional de ICANN y la creciente supervisión de sus actividades. La *Afirmación de Compromisos* sirvió de guía, pero dejó muchos asuntos por atender en los años venideros.

En noviembre de 2009, el cuarto IGF tuvo lugar en Sharm el Sheikh, Egipto. El tema central fue el futuro del IGF a la luz de la evaluación de 2010 del mandato del IGF. En sus presentaciones, los interesados brindaron una amplia gama de perspectivas sobre el futuro del IGF. Si bien la mayoría de ellos apoyaba la continuación del Foro, existían grandes diferencias de opinión en cuanto a la organización de futuros IGF. China y muchos de los países en vías de desarrollo abogaron por un anclaje más fuerte para el IGF en el sistema de la ONU, lo que implicaría un rol de mayor prominencia para los gobiernos. Los Estados Unidos, la mayoría de los países desarrollados, el sector comercial, y la sociedad civil abogaron por la preservación del modelo existente del IGF.

Desarrollos en 2010

El desarrollo más relevante de 2010 fue el impacto del crecimiento acelerado de las redes sociales en el debate sobre gobernanza de Internet, inclusive la protección de la privacidad de los usuarios de las plataformas de redes sociales como Facebook. En 2010, el principal desarrollo en la geopolítica de Internet fue el discurso de Hillary Clinton, la Secretaria de Estado de EE. UU., sobre la libertad de expresión en Internet, particularmente en relación con China.[10] Google y las autoridades chinas entraron en conflicto por el acceso restringido a las búsquedas de Google en China. Dicho conflicto llevó al cierre de las operaciones de búsqueda de Google en el país.

Existieron dos desarrollos importantes en el mundo de ICANN: (1) La introducción de los primeros dominios de nivel superior no ASCII para el árabe y el chino. Al resolver el problema de la disponibilidad de los dominios de nivel superior en escrituras no latinas, ICANN redujo el riesgo de desintegración del DNS de Internet. (2) La aprobación por parte de ICANN del dominio .xxx (contenido para adultos). Mediante esta decisión, la ICANN cruzó formalmente el Rubicón al tomar de manera oficial una decisión de gran relevancia para las políticas públicas de Internet. Anteriormente, la ICANN había intentado quedarse, al menos formalmente, dentro del ámbito de la toma de decisiones exclusivamente técnicas.

El proceso de revisión del IGF comenzó en 2010 con la Comisión de Ciencia y Tecnología para el Desarrollo de la ONU (CCTD) al adoptar la resolución para la continuación del IGF, la cual sugirió su continuidad por los siguientes cinco años, aplicando cambios mínimos en su organización y estructura. En julio de 2011, el Consejo Económico y Social de la ONU (ECOSOC) respaldó esta resolución, y la Asamblea General de la ONU tomó la decisión final sobre la continuación del IGF en el otoño.

Desarrollos en 2011

En 2011, el mayor desarrollo general fue el surgimiento de la gobernanza de Internet en la agenda política global. La relevancia de la gobernanza de Internet se acercó a otros asuntos diplomáticos, como el cambio climático, la migración, y la seguridad alimentaria. Otra consecuencia de la creciente relevancia política de Internet es la transición gradual de la cobertura nacional de los temas de gobernanza de Internet desde la tecnología (TI, telecomunicaciones) hacia los ministerios políticos (diplomacia, principales gabinetes de ministros). Además, los principales medios globales (por ejemplo, *The Economist, IHT, Al Jazeera, BBC*) comenzaron a seguir los desarrollos de la gobernanza de Internet más de cerca que nunca.

La gobernanza de Internet se vio afectada por la Primavera Árabe. Aunque existen muchos puntos de vista diferentes sobre el impacto de Internet sobre el fenómeno de la Primavera Árabe (que van desde lo insignificante hasta lo crucial), uno de los resultados es seguro: las redes sociales ahora se perciben como una herramienta que puede cumplir un rol decisivo en la vida política moderna. En varios sentidos, la Internet – y su gobernanza – apareció en los radares políticos a nivel mundial durante este año.

El 27 de enero, las autoridades de Egipto cortaron la Internet en un fallido intento por frenar las protestas políticas. Este fue el primer caso de un bloqueo de Internet en toda una nación llevado a cabo por el gobierno. Previamente, incluso en el caso de los conflictos militares (en la ex-Yugoslavia, Irak), la comunicación mediante Internet nunca había sido cortada en su totalidad.

La iniciativa de Hillary Clinton sobre la libertad de expresión en Internet, que tuvo comienzo en su discurso de febrero de 2010, se aceleró en 2011. Se llevaron a cabo dos conferencias importantes sobre este tema: la Conferencia de Viena sobre Derechos Humanos y la Internet, y la Conferencia de La Haya sobre Internet y Libertad.

En 2011, ICANN continuó su introspección con los siguientes desarrollos principales:

- La implementación de una reforma de gestión.
- Las preparaciones políticas finales para la introducción de nuevos dominios genéricos de nivel superior (gTLD).
- La búsqueda de un nuevo CEO.

El 2011 también fue marcado por una avalancha de nuevos principios de gobernanza de Internet propuestos por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), el Consejo de Europa, la UE, Brasil, y otras partes. Las numerosas convergencias de estos principios fueron consideradas como un posible punto de partida para un futuro preámbulo de una declaración global de Internet o un documento similar, que sirviera de marco para el desarrollo de la gobernanza de Internet.

Desarrollos en 2012

Fueron dos los eventos principales que marcaron la agenda de 2012 que tuvieron importantes consecuencias para los años próximos: el cambio de la directiva de ICANN, y la revisión del Reglamento de Telecomunicaciones Internacionales (RTI) de la UIT.

La ICANN había experimentado cambios significativos durante el año previo con la introducción de nuevos gTLD. Pese a algunos problemas con el proceso de registración (fallos técnicos en el *software*, controversias sobre el proceso de las políticas) se recibieron más de 1900 solicitudes para nuevos gTLD, que entraron en un proceso de evaluación y, a la larga, se decidió cuáles de estos se introducirían a la raíz a comienzos de 2014. Además, el nuevo CEO, Fadi Chehadé, aportó un nuevo enfoque para la dirección del proceso de políticas multilateral de ICANN. En su discurso dirigido a la sociedad civil en la reunión de ICANN 45, delineó algunas mejoras prometedoras en ICANN, que incluían el desarrollo de un multilateralismo responsable, el reconocimiento sincero de problemas, una escucha activa, una guía comprensiva, la búsqueda de términos medios, etc.

La Conferencia Mundial de Telecomunicaciones Internacionales (CMTI) se reunió en Dubái en diciembre de 2012 para modificar el RTI por primera vez desde 1988. Esto se llevó la mayor parte de la atención y planteó preocupaciones y debates sobre el impacto de una nueva regulación para el futuro de Internet. Al cabo de dos arduas semanas de conferencia, las negociaciones llegaron a un callejón sin salida: los participantes no lograron llegar a un consenso sobre el texto modificado, lo que dejó abierto el debate para las siguientes reuniones. El punto más polémico fue una resolución sin carácter vinculante sobre la promoción del rol de la UIT en la gobernanza de Internet, que provocó una polarización de los estados participantes en dos bloques: los países occidentales favorecieron el modelo existente de multilateralismo, mientras que aquellos que apoyaban la resolución, incluidos los estados de China, Rusia, y los países Árabes, se inclinaron hacia un modelo intergubernamental.

Otros desarrollos notables se registraron en el área de la propiedad intelectual, en la que la movilización y las protestas de los usuarios de Internet lograron bloquear las regulaciones nacionales (Acta de Cese de Piratería en Línea [SOPA] en EE. UU.) e internacionales (Acuerdo Comercial Anti-falsificación [ACTA]), que hubieran afectado los legítimos derechos de los usuarios mediante su implementación.

Desarrollos en 2013

El mayor suceso en las políticas digitales globales fueron las revelaciones de Snowden sobre los varios programas de vigilancia dirigidos por la Agencia de Seguridad Nacional de EE. UU. (NSA, por sus siglas en inglés) y otras. Las revelaciones de Snowden captaron el interés del público global sobre la manera en que se gobierna la Internet. El foco principal estuvo en la cuestión del derecho a la privacidad y la protección de datos.

Muchos líderes en la Asamblea General de la ONU (AGONU) abordaron la cuestión de la protección de la privacidad. La resolución de la AGONU inició un nuevo proceso de políticas sobre la privacidad en línea. Este tema se debatiría a fondo en 2014 en el Consejo de Derechos Humanos de la ONU.

En octubre de 2013, la presidenta de Brasil, Dilma Rousseff, y el presidente de ICANN, Fadi Chehadé, iniciaron el proceso NETmundial. La gobernanza de Internet se convirtió en el tema central de conferencias académicas y en las actividades de investigación de los centros de estudios alrededor del mundo.

Desarrollos en 2014

El 2014 comenzó con el discurso del presidente de EE. UU., Barack Obama, sobre la vigilancia de la NSA. En tal discurso, el presidente utilizó repetidamente el término

«ciberataques», priorizando a la ciberseguridad en la agenda sobre seguridad (antes que el terrorismo).

El 14 de marzo, la Administración Nacional de Telecomunicaciones e Información (NTIA, por sus siglas en inglés) del Departamento de Comercio de EE. UU. anunció que pretendía trasladar su rol de administración sobre las funciones clave de los nombres de dominio a la comunidad global de múltiples partes interesadas. En ese momento, la NTIA supervisaba el desempeño de las funciones de la Autoridad de Asignación de Números Internet (IANA, por sus siglas en inglés), lo que incluye el mantenimiento de los registros de nombres de dominio y direcciones IP, entre otros parámetros cruciales. La NTIA también autorizó los cambios en el archivo de zona de raíz (una libreta global de direcciones de Internet), contando así con un mecanismo de seguridad superior. Este anuncio provocó un largo proceso de consulta y consolidación de propuestas, originalmente para ser completadas en 2015, pero que se extendió luego por el lapso de un año. Al mismo tiempo, también se introdujo un proceso que apuntó a la consolidación de los mecanismos de rendición de cuentas dentro de ICANN.

Emergieron tres foros de debate, dos de los cuales estuvieron relacionados con ICANN:

- Una plataforma /1net (en línea) iniciada por ICANN para conectar a los distintos entes y contribuir con los resúmenes de debates en otros foros, en particular para el proceso NETmundial. La conferencia NETmundial (organizada de manera conjunta por /1net y el Comité Gestor de Internet en Brasil [CGI.br]) tuvo lugar durante el 23 y 24 de abril en San Pablo. Esta conferencia resultó en la Declaración NETmundial de Múltiples Actores Interesados, que contenía un conjunto de principios de gobernanza de Internet, así como también un camino a seguir para la futura evolución del ecosistema de la gobernanza de Internet.

- El panel de Alto Nivel sobre Corporación Global y Mecanismo de Gobernanza de Internet (GICGM, por sus siglas en inglés) se constituyó a partir de una sociedad entre ICANN y el Foro Económico Mundial (FEM), con la asistencia del Retiro de Annenberg en Sunnylands. El panel elaboró un informe al que llamaron Hacia un ecosistema de gobernanza de Internet colaborativa y descentralizada, el cual brindó una serie de recomendaciones para los avances de un ecosistema de gobernanza de Internet colaborativa y descentralizada.

- La Comisión Global sobre la Gobernanza de Internet fue lanzada por el Centro para la Innovación en Gobernanza Internacional de Canadá y el centro de estudio situado en el Reino Unido, Chatham House, con el objetivo de impulsar una visión estratégica para el futuro de la gobernanza de Internet.

El 3 de mayo se introdujo el «derecho al olvido» por parte del Tribunal de Justicia de la Unión Europea, cuyo fallo estableció que Google debía eliminar enlaces a datos personales «desactualizados», «excesivos», e «irrelevantes» cuando así lo requiriera un individuo que tuviera relación con los resultados de búsqueda desplegados bajo su nombre.

Desarrollos en 2015

A lo largo del año, la transición de la administración de IANA y la rendición de cuentas de ICANN permanecieron como temas centrales, mientras que el proceso se extendió a septiembre de 2016. La ciberseguridad continuó siendo prioridad en la agenda, tanto para

vulneraciones en la seguridad como para respuestas políticas. Tras deducir a comienzos del 2013 que las leyes internacionales existentes aplicaban al uso de las TIC por parte de los estados, el Grupo de Expertos Gubernamentales sobre los Avances en el campo de la Información y las Telecomunicaciones en el Contexto de Seguridad Internacional de la ONU (GGE) estuvo de acuerdo con varias normas, inclusive con no atacar a la infraestructura crítica o a los Equipos de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés). También se comprometió a asistir a otras naciones en la investigación de ciberataques y cibercrimen en sus territorios.

En julio, como parte de un proceso de objetivos de desarrollo sostenible (SDG, por sus siglas en inglés), la ONU estableció un nuevo Mecanismo de Facilitación Tecnológica[11], el cual comprende un equipo de trabajo interinstitucional de la ONU sobre ciencia, tecnología, e innovación; un foro de múltiples actores interesados; y una nueva plataforma de «mapeo» en línea. A partir de los debates del Consejo de Derechos Humanos, se acordó un mecanismo especial para el derecho a la privacidad y se designó al primer Relator Especial sobre Privacidad (el profesor Joseph Cannataci) el 3 de julio.

El verano también marcó el comienzo del proceso de revisión de la CMSI+10, que culminó en diciembre con la Reunión de Alto Nivel de la Asamblea General sobre la revisión total de la implementación de los resultados de la CMSI. El documento de resultados que allí se adoptó renovó el mandato del IGF por otros diez años y recalcó la dirección del desarrollo para la siguiente década, reiterando los roles y las responsabilidades de los participantes de la Agenda de Túnez de 2005.

Dentro de la comunidad de ICANN, continuaron los trabajos para el desarrollo de la propuesta de transición de la administración de IANA, y la propuesta de rendición de cuentas de ICANN.

Desarrollos en 2016

El 2016 empezó con dos informes que plantearon una pregunta fundamental: ¿Cómo se pueden maximizar las oportunidades y minimizar los riesgos que la Internet trae aparejados? El Informe sobre el Desarrollo Mundial 2016, del Banco Mundial: *Digital Dividends*[12] argumentó que la Internet no brinda beneficios a la sociedad de manera automática. Se necesitan políticas, educación, y mucho más para asegurar que la Internet tenga un impacto positivo en la sociedad. El FEM emitió un informe más cauteloso sobre la fragmentación de Internet, que explicaba los riesgos que existen para la Internet global (en forma de fragmentación técnica, gubernamental, y comercial).[13]

Una polémica entre Apple y la Oficina Federal de Investigaciones de EE. UU. (FBI) permaneció en los titulares durante varios meses a lo largo del 2016, debido a que una orden judicial le solicitaba a Apple que asistiera al FBI a forzar la entrada a un iPhone que pertenecía a uno de los terroristas que había asesinado a 14 personas en San Bernardino, California, en diciembre de 2015. El debate retomó la vieja cuestión sobre el equilibrio entre la seguridad y los derechos humanos en el reino digital. Si bien el caso fue finalmente desechado (ya que el gobierno de EE. UU. argumentó haberse beneficiado con la ayuda de un tercero para entrar en el teléfono), los asuntos relacionados con el cifrado, la privacidad, y la seguridad continuaron siendo en el foco de atención durante el año.

En junio de 2016, la Comisión Global sobre la Gobernanza de Internet publicó el informe One Internet, en el que se detallan una serie de recomendaciones para los legisladores, la

industria privada, la comunidad técnica, y otros interesados, acerca de algunas modalidades para mantener una Internet saludable. Aborda aspectos como la promoción de una Internet segura, abierta y confiable; la seguridad de los derechos humanos para los ciudadanos digitales; la identificación de las responsabilidades del sector privado; la garantía de la estabilidad y resiliencia del núcleo de la infraestructura de Internet; y la mejora de la gobernanza de Internet multilateral.[14]

Por parte de ICANN, la primera parte del año se destacó por la presentación, al gobierno de EE. UU., de la propuesta de transición de la administración de IANA y la propuesta de rendición de cuentas de ICANN. Tras revisar las dos propuestas, la NTIA reconoció, en agosto de 2016, que estas reunían los criterios anunciados en marzo de 2014. Por lo tanto, la ICANN procedió con la implementación de las disposiciones de ambas propuestas, en especial la creación de Identificadores Técnicos Públicos, como subsidiaria de la ICANN, encargada de tomar el control del desempeño de las funciones de IANA, y el empoderamiento de la comunidad de la ICANN mediante la inclusión, dentro de los reglamentos de la ICANN, de algunas disposiciones que le confirieran más poderes a la comunidad para responsabilizar a la ICANN (al personal y a la Junta) por sus acciones. El 1 de octubre expiró el contrato entre el gobierno de EE. UU. y la ICANN, lo que provocó el traslado de la administración de las funciones de IANA a la comunidad global de Internet.

Afijos y términos: e- / virtual / ciber / digital / net

Los afijos (prefijos y sufijos) y términos e- / virtual / ciber / digital / net se utilizan para describir los distintos desarrollos en el campo de la Internet y las TIC. Se usan indistintamente. Todos ellos hacen referencia al fenómeno de Internet.

Sin embargo, la tendencia es usar «e-» para el comercio, «ciber» para el crimen y la seguridad, «digital» para divisiones de desarrollo, y «virtual» para los tipos de moneda, como Bitcoin. Algunos patrones de uso comenzaron a aparecer. Mientras que en el lenguaje cotidiano la elección de «e-/virtual/ciber/digital/net» es casual, en las políticas de Internet, el uso de estos ha comenzado a acarrear un mayor significado y relevancia.

Revisemos rápidamente su etimología y la manera en que se usan en las políticas de Internet.

La etimología de «ciber» se remonta a la Antigua Grecia, con el significado de «gobernante». El término llegó a nuestras épocas mediante el libro de Norbert Weiner *Cibernética*, que abordaba la gobernanza determinada por la información.[15] En 1984, William Gibson acuñó la palabra «ciberespacio» en la novela de ciencia ficción *Neuromancer*.[16] El aumento del uso del prefijo «ciber» sucedió posteriormente al crecimiento de Internet. A fines de la década de 1990, casi todo lo relacionado con la Internet era « ciber »: cibercomunidad, ciberley, cibersexo, cibercrimen, cibercultura, etc. Si se hablaba de la Internet, escuchabas « ciber ». A principios de la década del 2000, este término comenzó a desaparecer de manera gradual del uso masivo, y quedó presente únicamente en la terminología sobre seguridad.

El prefijo « ciber » se utilizó para denominar a la Convención de Cibercrimen del Consejo de Europa. Es, hasta hoy, el único tratado internacional en el campo de la seguridad de Internet. Actualmente, existe la Estrategia para el Ciberespacio de EE.

UU., la Agenda sobre Ciberseguridad Global de la UIT, la política de Ciberdefensa de la OTAN, el Centro de Excelencia de Ciberdefensa de Estonia...

El autor ciberpunk y columnista de *Wired*, Bruce Sterling dijo lo siguiente al respecto:

> *Creo que sé por qué los militares le llaman « ciber » – se debe a que la metáfora de defender una « batalla espacial » hecha de « ciberespacio » hace que sea más fácil para los contratistas conseguir subvenciones del Pentágono. Si lo llaman « ciberespacio » debido al paradigma alternativo de « redes, alambres, tubos y cables », entonces la NSA ha sido la dueña desde hace 50 años y las fuerzas armadas no pueden decir ni una palabra.*[17]

« E » es la abreviatura de « electrónico ». Obtuvo su primer uso, el más importante, mediante el comercio electrónico (*e-commerce*), como descripción de una temprana comercialización de la Internet. En la Agenda de Lisboa de la UE (2000), el prefijo más usado fue « e- ». También fue el principal en las declaraciones de la CMSI (Ginebra 2003; Túnez 2005). La implementación del seguimiento de la CMSI tiene como foco las líneas de acción que incluyen el gobierno, comercio, aprendizaje, salud, empleo, agricultura, y ciencia electrónicos. No obstante, el prefijo « e- » no está tan presente como solía estarlo. Incluso la UE se ha distanciado gradualmente del uso de este prefijo en los últimos tiempos.

Hoy en día, la UE trabaja para la implementación de una Estrategia de Mercado Único Digital.[18]« Digital » hace referencia al 1 y al 0: los dos dígitos que son la base del mundo de la Internet. Básicamente, todos los programas de software empiezan con estos dígitos. En el pasado, el término « digital » era usado principalmente en los círculos de desarrollo para presentar la brecha digital. Durante los últimos años, el término ha comenzado a conquistar el espacio lingüístico del campo de la Internet. Es probable que se mantenga como el principal prefijo de Internet. Jean-Claude Juncker, presidente de la Comisión Europea, utilizó el término « digital » 10 veces en su discurso inicial en el Parlamento Europeo, en el que presentó su plan de políticas para su mandato de cinco años. Además de la UE, Gran Bretaña ahora posee *diplomacia* digital; y un creciente número de misiones diplomáticas cuentan con una persona dedicada a asuntos *digitales,* que usualmente los cubre de manera trasversal.

El término « virtual » se refiere a la naturaleza intangible de la Internet. Establece la ambigüedad de ser tanto intangible como, potencialmente, inexistente. La realidad « virtual » podría referirse a una realidad intangible (algo que no se puede tocar), así como también a una realidad que no existe (una realidad falsa). Los académicos y los pioneros de Internet usaron la palabra « virtual » para realzar la novedad del Internet, y el surgimiento de un « mundo nuevo y valiente ». Debido a la ambigüedad del término, no aparece muy seguido en el lenguaje de las políticas ni en los documentos internacionales.

Actualmente, existe una tregua en la guerra por la dominancia de estos afijos y términos. Cada uno se ha abierto camino en su propio territorio, sin que exista una dominación multifuncional, como la que tenía « ciber » a fines de la década de 1990. Hoy en día, el prefijo « ciber » preserva su dominancia en materia de seguridad. Se prefiere el prefijo « e- » en el ámbito de los negocios. El término « digital » evolucionó desde el uso de cuestiones de desarrollo hacia un uso más amplio por parte del sector gubernamental. El uso de la palabra « virtual » prácticamente se ha abandonado.

Conjunto de Herramientas Cognitivas para la Gobernanza de Internet

Las verdades profundas se reconocen por el hecho de que lo contrario también es una verdad profunda, a diferencia de las trivialidades, en las que los contrarios son un absurdo.

Niels Bohr, Físico Atómico (1885–1962).

El Conjunto de Herramientas Cognitivas para la Gobernanza de Internet es una serie de herramientas para el desarrollo y el entendimiento de la argumentación de políticas. El núcleo de este conjunto comprende un marco de referencia que incluye percepciones de relaciones de causa y efecto, modos de razonamiento, valores, terminología, y jerga. Este marco de referencia determina cómo se enmarcan algunas cuestiones específicas y qué acciones deben llevarse a cabo.

En muchos casos, el marco de referencia común se ve influenciado por la cultura profesional específica (los patrones de conocimiento y comportamientos compartidos por los miembros de una misma profesión; por ejemplo, los diplomáticos, académicos, desarrolladores de *software*). La existencia de dicho marco usualmente ayuda a facilitar una mejor

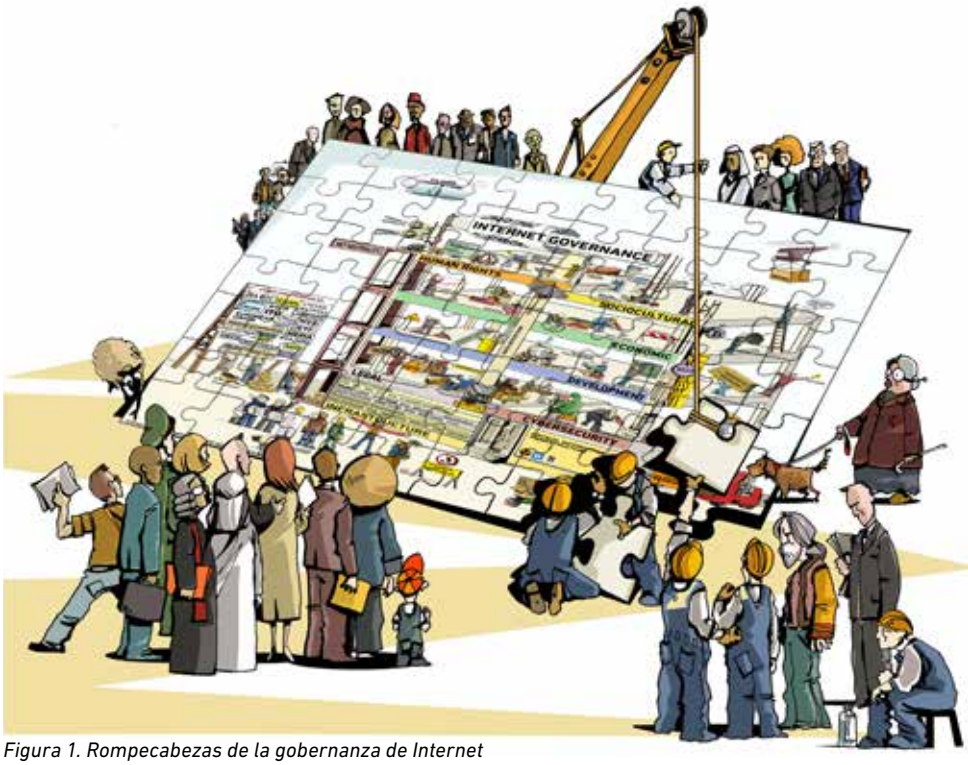

Figura 1. Rompecabezas de la gobernanza de Internet

comunicación y entendimiento. También se puede acudir a él para la protección del territorio profesional y la prevención de la influencia externa. Para citar a Jeffrey Mirel, lingüista estadounidense: « Todo lenguaje profesional es lenguaje territorial ».[19]

El régimen de la gobernanza de Internet es complejo, ya que comprende muchas cuestiones, actores, mecanismos, procedimientos, e instrumentos. La Figura 1, inspirada por el artista holandés MC Escher, demuestra algunas de las perspectivas paradójicas asociadas con la gobernanza de Internet.

El conjunto de herramientas refleja la naturaleza de la gobernanza de Internet, como un área política considerada malvada, caracterizada por la dificultad que se encuentra en la designación de causalidad para el desarrollo de políticas a una razón específica. En muchos casos, los problemas son síntomas de otros problemas, lo que crea a menudo círculos viciosos. Algunos enfoques cognitivos, como el lineal, el monocausal, y el pensamiento binario, tienen una utilidad muy limitada en el campo de la gobernanza de Internet. La gobernanza de Internet es demasiado compleja como para amarrarla dentro de un corsé de coherencia y consistencia, libre de contradicciones. La flexibilidad, y la apertura y preparación para lo inesperado, pueden ser la mejor parte de la Internet.[20]

Tal como el proceso de la gobernanza de Internet, el conjunto de herramientas también está en constante cambio. Los enfoques, patrones y analogías aparecen y desaparecen dependiendo de la relevancia que posean en cada momento en el proceso de políticas. Estos apoyan las narrativas de políticas específicas en el debate sobre la gobernanza de Internet.

Enfoques de política

La primera sección del Conjunto de Herramientas para la Gobernanza de Internet describe una serie de enfoques de política que sustentan las posiciones de los actores principales de la gobernanza de Internet. Estos enfoques de político también explican la formulación de posiciones de negociación y debates de política.

Enfoque limitado vs amplio

El enfoque limitado se concentra en la infraestructura de Internet (el DNS, los números IP, y los servidores raíz) y en la posición de ICANN como actor clave en este campo. Según el enfoque amplio, las negociaciones en la gobernanza de Internet deberían ir más allá de los problemas infraestructurales, y se deberían abordar cuestiones legales, económicas, socioculturales, y de desarrollo. Este último enfoque se adopta en el informe del GTGI y la Agenda de Túnez para la Sociedad de la Información. También se utiliza como principio subyacente en la arquitectura del IGF.

Sin embargo, existe una tendencia a considerar a la ciberseguridad y al comercio electrónico como campos de políticas separados de la gobernanza de Internet. Por ejemplo, el documento de revisión de la CMSI+10 de 2015[21] abordó la gobernanza de Internet y la ciberseguridad en capítulos separados. Enmarcar el debate de políticas digitales va mucho más allá de la simple pedantería académica. Abordar estas cuestiones en silos políticos (por ejemplo, la seguridad, los derechos humanos, el comercio electrónico) puede afectar la efectividad para enfrentar los asuntos de las políticas de Internet, que son por naturaleza multidisciplinarios. Muchos actores, desde gobiernos hasta organizaciones internacionales

y el sector comercial, hacen frente al problema de cómo pasar por alto esos silos y abordan los problemas de las políticas de Internet de una manera amplia y multidisciplinaria.

Coherencia Técnica y Política

Uno de los desafíos más importantes que enfrenta la gobernanza de Internet es el de cómo lidear con los aspectos técnicos y políticos, ya que es difícil realizar una clara distinción entre ambos. Las soluciones técnicas no son neutrales. A la larga, cada solución/opción técnica promueve intereses determinados, empodera a ciertos grupos, y, hasta cierto punto, tiene un impacto en la vida social, política, y económica. En el caso de Internet, durante mucho tiempo, tanto el aspecto técnico como el político estaban gobernados por un único grupo social: la comunidad técnica de Internet originaria.

Con el crecimiento de Internet y el surgimiento de nuevos actores en su gobernanza – más que nada del sector comercial y los gobiernos – fue difícil para la comunidad técnica de Internet mantener una cobertura integrada de los asuntos técnicos y políticos bajo un mismo techo. Las reformas subsiguientes, incluida la creación de ICANN, intentaron restablecer la coherencia entre los aspectos técnicos y políticos. Este tema continúa abierto, y como era de esperar, ha demostrado ser uno de los más controvertidos en el debate sobre el futuro de la gobernanza de Internet.

Enfoque « viejo y real » vs « nuevo y cibernético »

Existen dos enfoques para casi cualquier cuestión de gobernanza de Internet (Figura 2). El enfoque « viejo y real » sostiene que la Internet no introdujo nada nuevo al campo de la gobernanza. Desde la perspectiva de la gobernanza, el Internet es meramente otro elemento nuevo, que no se diferencia de sus predecesores: el telégrafo, el teléfono, y la radio.

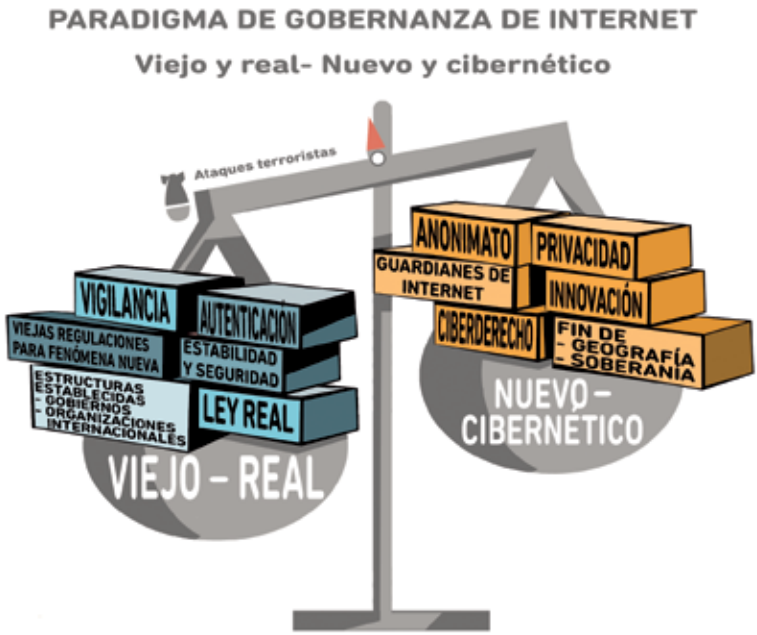

Figura 2. Paradigma de la gobernanza de Internet

Por ejemplo, en los debates legales, este enfoque mantiene que las leyes existentes se pueden aplicar a Internet con solo unos mínimos cambios. En cuanto a lo económico, este enfoque afirma que no existe diferencia alguna entre el comercio común y el electrónico. Por lo tanto, no hay necesidad de que exista un tratamiento legal especial para el comercio electrónico.

El enfoque « nuevo y cibernético » señala que la Internet es un sistema de comunicación fundamentalmente diferente de todos los anteriores. La premisa principal del enfoque cibernético es que la Internet ha logrado desvincular nuestra realidad política y social del mundo físico, delimitado por territorios estatales soberanos separados geográficamente. El ciberespacio difiere del espacio real y exige una forma de gobernanza distinta. Esta opinión de que el ciberespacio es un espacio nuevo y diferente está respaldada por una decisión que tomó la OTAN en la Cumbre de Varsovia de 2016 al declarar que el ciberespacio sería el cuarto dominio operacional militar, para sumarse a los dominios de tierra, agua, y aire. [22]

En el campo legal, la escuela del pensamiento cibernético sostiene que las leyes existentes sobre jurisdicción, delito, y contratos no se pueden aplicar a Internet y que se deben promulgar nuevas leyes. El enfoque « viejo y real » está volviéndose cada vez más importante tanto en el campo de trabajos regulatorios como en el de políticas. El GGE de la ONU reafirmó el punto de vista que mantiene que el derecho internacional existente aplica al uso de las TIC por parte de los estados. Además, numerosas convenciones sobre derechos humanos de la ONU han aceptado el principio de que los derechos humanos fuera de línea aplican también en línea.

Estructura de gobernanza de Internet descentralizada vs centralizada

Según el punto de vista de la descentralización, la gobernanza de Internet debería reflejar la naturaleza esencial de Internet: una red de redes. Esta opinión hace hincapié en que la Internet es tan compleja que no se puede ubicar bajo un solo paraguas de gobernanza, como una organización internacional, y subraya que la gobernanza descentralizada es uno de los principales factores que permite el rápido crecimiento de Internet. Esta línea de pensamiento está respaldada más que nada por la comunidad técnica de Internet y por los países desarrollados.

El enfoque centralizado aboga por un centro único para el abordaje de cuestiones de la gobernanza de Internet, preferentemente dentro del marco de una organización internacional. Una de las motivaciones más importantes para el enfoque de una gobernanza más centralizada es la dificultad que enfrentan los países con recursos humanos y financieros limitados para el seguimiento de los debates sobre gobernanza de Internet en un ambiente altamente descentralizado y multinstitucional. Para estos países es difícil asistir a las reuniones en los principales centros diplomáticos (Ginebra, Nueva York), y es aún más difícil para ellos es seguir las actividades de otras instituciones, como ICANN, el Consorcio World Wide Web (W3C), e IETF.

Protección de los intereses públicos en Internet

Una de las principales fortalezas de la Internet es su apertura y su naturaleza pública, lo que ha permitido su rápido crecimiento y promueve la creatividad e inclusión. La manera de proteger esta naturaleza pública de la Internet permanecerá como uno de los temas

centrales en los debates sobre su gobernanza. Este problema es especialmente intrincado dado que una parte sustancial de la infraestructura de base de Internet – desde las conexiones troncales transcontinentales a las redes de áreas locales – es de propiedad privada. Algunas de las difíciles preguntas que necesitan respuesta tienen que ver con si se les debería solicitar a los dueños privados que administren esta propiedad en el interés público, y con la delimitación de las partes de Internet que se pueden considerar un bien público. Por ejemplo, el investigador holandés Dennis Broeders[23] y el embajador maltés, el Dr. Alex Sceberras Trigona[24] , fomentaron el pensamiento de que la infraestructura básica de Internet debería considerarse como un recurso público global. Ha resurgido la pregunta sobre la naturaleza pública de Internet mediante el debate sobre la neutralidad de la red.

Consulte la Sección 7 para obtener más información acerca del debate sobre los bienes públicos globales.

Geografía e Internet

Una de las suposiciones prematuras sobre Internet fue que traspasaba los límites nacionales y erosionaba el principio de soberanía. Con la comunicación de Internet trascendiendo fácilmente los límites nacionales y la autonomía del usuario integrada en el propio diseño de Internet, a muchos les pareció que, citando la famosa Declaración de independencia del ciberespacio[5], los gobiernos « no tienen derecho moral a gobernarnos [a los usuarios] ni poseen métodos para hacernos cumplir su ley que debamos temer verdaderamente».

Los desarrollos tecnológicos de los últimos tiempos, incluido el *software* de geolocalización de mayor sofisticación, cuestionan cada vez más la postura que apoya el fin de la geografía en la era de Internet. Por el contrario: marcan el regreso de la geografía. Los usuarios de Internet están más anclados en la geografía que en la era previa a Internet. Como consecuencia, mientras más anclada a la geografía esté la Internet, menos única será su gobernanza. Por ejemplo, con la posibilidad de localizar geográficamente a las transacciones y a los usuarios de Internet, se puede resolver la compleja pregunta sobre la jurisdicción de Internet, mediante las leyes existentes.

Tecnología digital e incertidumbre política

La tecnología digital se desarrolla muy rápidamente. Casi todos los días se introducen nuevos servicios. Esto provoca más dificultades a la hora de organizar el debate sobre la gobernanza de Internet. Por ejemplo, en noviembre de 2005, cuando el acuerdo actual de la gobernanza de Internet se negoció en la CMSI en Túnez,[25] Twitter todavía no existía. Hoy, el uso de Twitter ha impulsado algunos de los asuntos centrales de gobernanza de Internet, como la protección de la privacidad y la libertad de expresión.

La lucha contra el correo no deseado (spam) es otro ejemplo de cómo la tecnología tiene un impacto sobre la gobernanza de Internet. En 2005, el spam era uno de los asuntos clave de la gobernanza. Hoy en día, gracias a los filtros tecnológicos altamente sofisticados, el correo no deseado es un asunto que no posee gran prominencia en la gobernanza de Internet.

Por lo tanto, algunos de los problemas de política actuales podrían ser resueltos como consecuencia de los desarrollos tecnológicos.

Actos de equilibrio de políticas

El equilibrio es, probablemente, la visualización más apropiada en lo que respecta a la gobernanza de Internet y los debates sobre políticas. En muchos de los asuntos de la gobernanza de Internet, debe establecerse un equilibrio entre varios intereses y enfoques. Establecer este equilibrio es, a menudo, la base para llegar a los consensos. Las áreas de equilibrio de políticas incluyen:

- La libertad de expresión vs la protección del orden público: el reconocido debate sobre el Artículo 19 (la libertad de expresión) y el Artículo 29 (la protección del orden público) de la Declaración Universal de los Derechos Humanos ha llegado hasta el campo de la Internet. Se debate frecuentemente en el contexto del control de contenidos y censura en Internet.

- Ciberseguridad vs privacidad: al igual que la seguridad en la vida real, la ciberseguridad puede poner en peligro algunos derechos humanos, como el derecho a la privacidad. El equilibrio entre la ciberseguridad y la privacidad sufre cambios constantemente, dependiendo de la situación política global general. Debido a los ataques terroristas que colocaron el tema de la seguridad en la agenda global, el equilibrio se ha inclinado hacia la ciberseguridad.

Consulte la Sección 3 para obtener más información acerca del debate sobre ciberseguridad.

- Propiedad intelectual: la protección de los derechos de autor vs el uso justo de materiales es otro dilema de ley « real » que ha llevado una nueva perspectiva al mundo en línea.

Consulte la Sección 4 para obtener más información acerca del debate sobre la propiedad intelectual.

Muchos critican estos pares de equilibrios, ya que los consideran falsos dilemas. Por ejemplo, existen argumentos sólidos que afirman que un incremento en la ciberseguridad no significa necesariamente una disminución de la privacidad. Existen enfoques para mejorar ambas. Mientras que estas opiniones se mantienen firmes, la realidad de la política de la gobernanza de Internet es que esta se moldea mediante la búsqueda de soluciones equilibradas, y en la identificación de términos medios entre las varias opciones políticas.

No reinventes la rueda

Todas las iniciativas en el campo de la gobernanza de Internet deberían comenzar por las regulaciones y/o políticas existentes, que se pueden dividir en dos grandes grupos:

- Aquellas que fueron inventadas para Internet (por ejemplo, las políticas de ICANN sobre la administración de los nombres y números de Internet, las regulaciones sobre la neutralidad de la red, las políticas en el campo del Internet de las Cosas).

- Las políticas y regulaciones ya instauradas requieren modificaciones para poder abordar las especificidades relacionadas con Internet. El nivel de modificaciones varía desde ajustes limitados, como en el campo de los derechos humanos, hasta modificaciones más profundas en cuanto a la regulación, por ejemplo, de cibermonedas e impuestos electrónicos.

El uso de las reglas existentes representaría un incremento significante en la estabilidad legal y una reducción de la complejidad de los desarrollos de futuros regímenes políticos digitales.

Si no está roto, no lo arregles

La gobernanza de Internet debe mantener la actual funcionalidad y robustez de Internet y a la vez poseer la flexibilidad suficiente como para adoptar cambios que lleven a un incremento de su funcionalidad y una legitimidad superior. El consenso general reconoce que la estabilidad y funcionalidad de Internet deben estar entre los principios rectores de la gobernanza de Internet.

La estabilidad de Internet se ha preservado mediante el uso del prematuro enfoque de Internet de « el código que funciona », que comprende la introducción gradual de cambios comprobados en la infraestructura técnica. Sin embargo, a algunos actores les preocupa que el uso del eslogan « si no está roto, no lo arregles » provea una manta de inmunidad de cualquier cambio en la gobernanza de Internet actual, incluidos aquellos cambios que no están necesariamente relacionados con la infraestructura técnica. Una solución es el uso de este principio como criterio para la evaluación de decisiones relacionadas específicamente con la gobernanza de Internet (por ejemplo, la introducción de nuevos protocolos y cambios en los mecanismos de toma de decisiones).

Promover un enfoque y una priorización holísticos

Un enfoque holístico facilitaría el abordaje no solo de los aspectos técnicos de Internet, sino también de las dimensiones legales, económicas, de desarrollo, seguridad, y derechos humanos. Este enfoque debería también tener en cuenta la creciente convergencia de la tecnología digital, con las compañías de Internet que se trasladan al mercado de la telecomunicación (por ejemplo, Google y Facebook, en el uso del cableado submarino), y las compañías de telecomunicaciones que proveen servicios de contenidos digitales.

En el mantenimiento del enfoque holístico en lo que respecta a las negociaciones de la gobernanza de Internet, los actores interesados deberían identificar los asuntos de prioridad dependiendo de sus intereses particulares, como las ramas de un « árbol » que ellos elijan, sin perder de vista el bosque en el que se encuentran los asuntos de la gobernanza de Internet (Figura 3).

Ni los países en vías de desarrollo ni los desarrollados son grupos homogéneos. Entre los países en vías de desarrollo, existen diferencias importantes en las prioridades, nivel de desarrollo, y la disponibilidad TI (por ejemplo, entre los países avanzados en las TIC, como la India, China, y Brasil, y algunos países menos desarrollados como África Subsahariana).

Un enfoque y una priorización holísticos de la agenda de la gobernanza de Internet deberían ayudar a los actores interesados tanto de los países desarrollados como de los países en vías de desarrollo a centrarse en un conjunto de asuntos determinado. Esto debería desembocar en negociaciones más sustantivas y, posiblemente, menos politizadas. Las partes interesadas se agruparían con respecto a estos asuntos en lugar de agruparse en torno a la línea de divisiones tradicional sumamente politizada (por ejemplo, países desarrollados/en vías de desarrollo, sociedad civil/gobiernos).

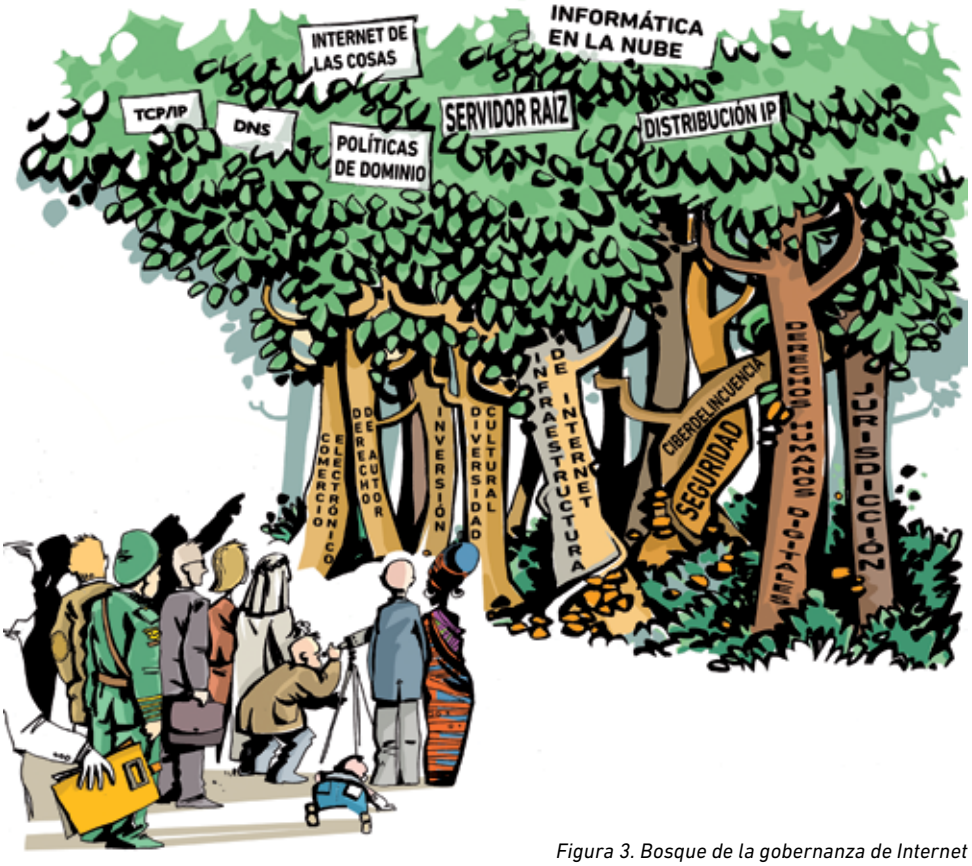

Figura 3. Bosque de la gobernanza de Internet

La neutralidad tecnológica

Según el principio de la neutralidad tecnológica, la política no debe diseñarse en torno a tecnologías o dispositivos específicos. Por ejemplo, las regulaciones para la protección de la privacidad deberían especificar qué proteger (por ejemplo, los datos personales, las historias médicas), y no cómo protegerlos (por ejemplo, el acceso a las bases de datos, la protección mediante cifrado).

La neutralidad tecnológica brinda muchas ventajas gubernamentales. Asegura la continua relevancia de la gobernanza sin perjuicio de los futuros desarrollos tecnológicos y posible convergencia de las tecnologías principales (la telecomunicación, los medios, la Internet, etc.). La neutralidad tecnológica difiere de la neutralidad en la red: la primera indica que la política particular es independiente de la tecnología que regula, mientras que la última se concentra principalmente en la neutralidad del tráfico de Internet.

Soluciones técnicas como políticas tácitas

Un pensamiento común dentro de la comunidad de Internet se basa en que ciertos valores sociales, como la libre comunicación, se ven facilitados por el diseño técnico de Internet. Por ejemplo, el principio de neutralidad de la red, que señala que la red debería simplemente transmitir

datos entre dos extremos sin discriminar el tráfico de ninguna manera, se considera a menudo como una de las salvaguardas técnicas de la libertad de comunicación en Internet. Esta postura podría resultar en la conclusión errónea de que las soluciones tecnológicas son suficientes para la promoción y protección de los valores sociales. Algunas otras soluciones, como la del uso de tecnologías de contrafuego para la restricción del flujo de información, demuestran que la tecnología puede ser usada de muchas formas, aparentemente contradictorias. Cuando sea posible, los principios como la libre comunicación deberían quedar claramente establecidos a nivel político, y no asumidos de manera tácita a nivel técnico. Las soluciones tecnológicas deberían fortalecer los principios políticos, pero sin ser la única manera de promoverlos.

El manejo de la sociedad mediante algoritmos

Uno de los aspectos clave de la relación entre la tecnología y las políticas fue identificado por el académico estadounidense Lawrence Lessig, quien observó que, con su creciente dependencia de la Internet, la sociedad moderna podría acabar regulándose por medio de códigos de *software* en lugar de reglas legales. En última instancia, algunas de las funciones de los parlamentos, gobiernos, y tribunales podrían ser desempeñadas *de facto* por compañías informáticas y desarrolladores de *software*. Mediante una combinación de soluciones técnicas y de *software*, serían capaces de influenciar la vida de las sociedades cuya relación con la Internet es cada vez más estrecha. Se espera que un nuevo conjunto de tecnologías basadas en la Inteligencia Artificial (IA) transfiera algunas decisiones humanas hacia las máquinas. Uno de los debates más acalorados actualmente tiene que ver con la futura regulación de los automóviles sin conductor. La sociedad moderna tendrá que ser capaz de identificar y lidiar con la línea divisoria entre las máquinas que remplazan a humanos en actividades diarias, y las que se encuentran en el reino de la toma de decisiones relacionadas con la organización política y judicial de nuestra sociedad.

Analogías

Aunque la analogía es a menudo engañosa, es lo menos engañoso que tenemos.

Samuel Butler, poeta inglés (1835–1902)

La analogía nos ayuda a comprender nuevos desarrollos haciendo referencia a lo que ya es conocido. Establecer paralelos entre ejemplos pasados y actuales, a pesar de ser riesgoso, es uno de los procesos cognitivos clave del derecho y la política. La mayoría de los casos legales relativos a la Internet se resuelven mediante analogías, especialmente en el sistema legal anglosajón basado en precedentes. El uso de las analogías en la gobernanza de Internet tiene algunas limitaciones importantes.

Primero que nada, el término « Internet » es amplio; abarca una amplia variedad de servicios, en los que se encuentran el correo electrónico (análogo al teléfono), los servicios web (análogos a los servicios de radiodifusión y televisión), las bases de datos (análogas a las bibliotecas), y las plataformas de redes sociales (análogas a las cafeterías o los bazares). Una

analogía basada en un aspecto particular de Internet puede reducir la comprensión de la Internet a aspectos limitados.

En segundo lugar, con la creciente convergencia de distintos servicios de telecomunicaciones y de medios, las diferencias tradicionales entre estos servicios se vuelven difusas. Por ejemplo, con la introducción del VoIP, es cada vez más difícil hacer la distinción entre la Internet y la telefonía. A pesar de estos factores restrictivos, las analogías son, aun así, poderosas; son todavía la principal herramienta cognitiva para resolver casos legales y desarrollar un régimen de gobernanza de Internet.

En tercer lugar, las analogías fueron de gran importancia en las etapas tempranas de Internet, momento en el que se trataba no solo de una herramienta nueva sino también de un fenómeno. Por ejemplo, en la primera edición de este libro (2004), las analogías cumplieron un papel esencial en la explicación de la Internet. Con el crecimiento de esta, las analogías se han vuelto menos relevantes. Las generaciones jóvenes están creciendo a la par de la Internet. Para ellas, algunas analogías en este estudio (como la videograbadora – VCR) pueden parecer anticuadas. De todas formas, las analogías siguen siendo la base de muchas resoluciones judiciales y políticas sobre Internet que han sido las responsables de moldear la gobernanza de Internet. Por lo tanto, el siguiente resumen de analogías tiene como propósito servir tanto de registro histórico del uso de las analogías en la gobernanza de Internet, como de una herramienta para la interpretación de las raíces de desarrollos actuales en las políticas digitales.

Internet – telefonía

Similitudes: durante los primeros días de la Internet, esta analogía se vio influenciada porque el teléfono se usaba para acceder a la Internet mediante el marcado. Además, existe una analogía funcional entre el teléfono y la Internet (correo electrónico y charlas), ya que ambos son medios de comunicación directa y personal.

Diferencias: la telefonía análoga usaba circuitos, mientras que la Internet usa paquetes. A diferencia de la telefonía, la Internet no puede garantizar servicios; solamente garantiza su « mejor esfuerzo ». La analogía resalta únicamente un aspecto de la Internet: la comunicación mediante correo electrónico o chat. Otras aplicaciones importantes de Internet, como World Wide Web, servicios interactivos, etc., no comparten elementos en común con la telefonía.

Utilización: Aquellos que se oponen a la regulación del contenido de Internet usan esta analogía. Si la Internet es análoga al teléfono, el contenido de las comunicaciones de Internet no se puede controlar judicialmente, como sucede con, por ejemplo, la radiodifusión. A esta analogía también la utilizan aquellos que afirman que la Internet debería estar gobernada como otros sistemas de comunicación (por ejemplo, la telefonía o el correo), por las autoridades nacionales, con el papel coordinador de las organizaciones internacionales, como la UIT. Según esta analogía, el DNS de Internet debería estar organizado y administrado como el sistema de numeración de la telefonía.[26]

Los servicios VoIP (como Skype) que desempeñan la función del teléfono usando números de protocolos de Internet crearon un nuevo giro en esta compleja analogía. Esta dicotomía propulsó una controvertida política en el Congreso Mundial de Tecnologías de la Información (WCIT, por sus siglas en inglés) de 2012 en Dubai. La opinión actual acerca de que el VoIP es un servicio de Internet se ve desafiada por aquellos que afirman que el servicio debería estar regulado como el de la telefonía tanto a nivel nacional como internacional, y que se le debería otorgar un rol más prominente a la UIT.

Internet – Correo tradicional/postal

Similitudes: esta analogía tiene su base en una función en común, específicamente la de la entrega de mensajes. El propio nombre – correo electrónico – pone de relieve esta similitud.

El sistema postal y ICANN

Paul Twomy, exdirector ejecutivo de ICANN, utilizó la siguiente analogía entre el sistema postal y la función de ICANN: « Si uno piensa en la Internet como una oficina de correo o un sistema postal, la designación de nombres de dominio y dirección IP esencialmente aseguran que la dirección que se encuentra en el sobre, funcione. No se trata de lo que se encuentra dentro del sobre, quién lo envía, quién tiene derecho a leerlo, cuánto demora en llegar, o cuál es el precio de ese sobre. Ninguna de estas cuestiones importa bajo las funciones de ICANN. La función se concentra solamente en asegurar que la dirección funcione ».

Diferencias: esta analogía cubre exclusivamente uno de los servicios de Internet: el correo electrónico. Además, el servicio postal tiene una estructura intermediaria mucho más elaborada entre el remitente y el destinatario que la del sistema de correo electrónico, en el que la función intermediaria activa es llevada a cabo por los PSI o por un proveedor de servicios de correo electrónico como Yahoo! O Hotmail.

Utilización: el Convenio Postal Universal define al correo electrónico de la siguiente manera: « es un servicio postal que comprende la transmisión electrónica de "mensajes" ». Esta analogía puede tener consecuencias con respecto a la entrega de documentos oficiales. Por ejemplo, la recepción de una orden judicial mediante un correo electrónico podría considerarse como una entrega oficial.

Las familias de los soldados estadounidenses que murieron en Irak también intentaron hacer uso de la analogía entre el correo postal (las cartas) y el correo electrónico, con el objetivo de obtener acceso a los correos electrónicos y *blogs* de sus seres queridos, alegando que deberían estar autorizados a heredar los correos electrónicos y *blogs* de la misma manera en que heredarían sus cartas y agendas. Para los PSI es difícil lidiar con este problema con alto contenido emocional. En lugar de seguir la corriente de esta analogía entre las cartas y los correos electrónicos, la mayoría de los PSI denegaron el acceso, basándose en el acuerdo de privacidad que firmaron con sus usuarios.

Internet – televisión

Similitudes: la analogía inicial tiene que ver con la similitud física entre las pantallas de las computadoras y de los televisores. Una analogía más sofisticada se basa en el uso de ambos medios – la web y la TV – con respecto a la difusión.

Diferencias: la Internet es un medio más amplio que la televisión. Además de la similitud entre la pantalla de una computadora y la de un televisor, existen diferencias estructurales fundamentales. La televisión es un medio de difusión « uno a muchos » en cuanto a la difusión para los televidentes, mientras que Internet facilita muchos tipos de comunicación distintos (uno a uno, uno a muchos, muchos a muchos).

Utilización: aquellos que quieren implementar un control más estricto sobre la Internet hacen uso de esta analogía. Desde esa perspectiva, debido al poder de Internet como una herramienta de comunicación masiva similar a la televisión, la Internet debería estar controlada de manera estricta. El gobierno de EE. UU. intentó usar esta analogía en el caso ejemplar *Reno vs la Unión Estadounidense por las Libertades Civiles*.[27] Este caso fue suscitado por la Ley de Decencia en las Comunicaciones aprobada por el Congreso, que estipula un control de contenidos estricto con el propósito de evitar que los niños queden expuestos a contenido pornográfico vía Internet. La corte se rehusó a reconocer la analogía de la televisión.

Internet – biblioteca

Similitudes: a veces se considera que la Internet es un vasto depósito de información, y el término « biblioteca » se usa a menudo para describirla: por ejemplo, « una enorme biblioteca digital », « una ciberbiblioteca », « la biblioteca de Alejandría del siglo XXI », etc.

Diferencias: el almacenamiento de información y datos es solo uno de los aspectos de Internet, y existen diferencias considerables entre las bibliotecas y la Internet:

- Las bibliotecas tradicionales apuntan a brindar un servicio para los individuos que viven en un lugar en particular (ciudad, país, etc.), mientras que la Internet es global.

- Los libros, artículos y periódicos se publican tras procedimientos que aseguran su calidad (editores). Normalmente, la Internet no siempre cuenta con editores.

- Las bibliotecas están organizadas a partir de esquemas de clasificación específicos, que permiten a los usuarios localizar los libros que se encuentran en sus colecciones. Este tipo de esquema de clasificación generalizada de información no se existe en Internet.

- Aparte de las descripciones mediante palabras clave, no se puede acceder a los contenidos de las bibliotecas (los textos dentro de los libros y artículos) hasta que el usuario pide prestado un libro o periódico en particular. En cambio, se puede acceder al contenido de Internet inmediatamente mediante los motores de búsqueda.

Utilización: esta analogía es utilizada en varios proyectos que tienen como objetivo crear un sistema holístico de información y conocimiento acerca de temas específicos (portales, bases de datos, etc.). La analogía de la biblioteca ha sido utilizada en el contexto de un proyecto de libro de Google con el propósito de digitalizar todos los libros en soporte papel.

Internet – videograbadora, fotocopiadora

Similitudes: esta analogía se concentra en la reproducción y diseminación de contenido (por ejemplo, de textos y libros). Las computadoras simplificaron la reproducción mediante el proceso de « copiar y pegar ». Esto, a su vez, hizo que la diseminación de la información a través de Internet fuera mucho más simple.

Diferencias: las computadoras tienen una función mucho más amplia que la de copiar materiales, aunque esta acción es mucho más simple en Internet que con una videocasetera o una fotocopiadora.

Utilización: se utilizó esta analogía en el contexto de la Ley de Derechos de Autor de la Era Digital (DMCA, por sus siglas en inglés), que sanciona a las instituciones que contribuyan con la violación del derecho de autor (en el desarrollo de *software* para el rompimiento de la protección del derecho de autor, etc.). El contraargumento en estos casos era que los desarrolladores de *software,* como los fabricantes de videograbadoras y fotocopiadoras, no pueden predecir si sus productos se usarán ilegalmente.

Esta analogía se utilizó en muchos casos contra los desarrollares de *software* al estilo de Napster para compartir archivos entre pares (P2P), como Grokster y StreamCast.

Internet – autopista

Similitudes: la autopista es al transporte en el mundo real, lo que la Internet para la comunicación en el espacio virtual.

Diferencias: además del aspecto de Internet de la transportación de datos, no existen otras similitudes entre esta y la autopista. Internet traslada materiales intangibles (datos), mientras que las autopistas facilitan la transportación de bienes y personas.

Utilización: la analogía de la autopista se usó extensivamente a mediados de la década de 1990, luego de que Al Gore acuñara, supuestamente, el término « superautopista de la información ». La palabra « autopista » también se utilizó en el gobierno alemán para justificar la introducción de una ley de control de contenidos más estricta en junio de 1997:

> *Se trata de una ley liberal que no tiene ninguna relación con la censura, sino que establece claramente las condiciones de lo que es posible o no para un proveedor. Internet es un medio de transporte y distribución de conocimiento... al igual que las carreteras, es necesario tener pautas para ambos tipos de tráfico.*[28]

Las autopistas e Internet

Hamadoun Touré, Secretario General de la UIT, usó una analogía entre las autopistas e Internet, estableciendo una relación entre las autopistas y la telecomunicación, y el tráfico de Internet y los camiones o automóviles: « Estaba dando un simple ejemplo de la comparación entre Internet y las telecomunicaciones y camiones, automóviles y las autopistas. Ser dueño de las autopistas no significa ser dueño de todos los camiones o automóviles que viajan por ellas, y ciertamente tampoco de los bienes que transportan, y vice versa. Es una analogía simple. Sin embargo, para que el tráfico pueda moverse sin contratiempos, uno, a medida que construye las carreteras, necesita conocer el peso, la altura y la velocidad de los camiones, para poder construir los puentes apropiados. De lo contrario, el sistema no funcionará con fluidez. En mi opinión, esa es la relación entre Internet y el mundo de la telecomunicación. Están destinados a trabajar juntos. »[29]

Internet – alta mar

Similitudes: en un principio, se estableció una analogía entre las aguas de alta mar y el tráfico de Internet, que parecía traspasar las jurisdicciones nacionales.

Diferencias: no hay ningún aspecto que coincida entre la Internet y las aguas de alta mar. En primer lugar, los datos de Internet quedan siempre dentro del reino de alguna jurisdicción nacional. El cableado de telecomunicaciones en el lecho marino puede yacer en los lechos de alta mar en el Océano Pacífico y en el Atlántico, pero son posesión de, predominantemente, compañías privadas, que están sujetas a las jurisdicciones nacionales en las que se incorporan legalmente. En caso de que Microsoft coloque centros de datos en alta mar (algo que ya ha estado considerando la compañía), estarán sujetos a la jurisdicción estadounidense, ya que Microsoft está incorporada en EE. UU. Cualquier dispositivo, cable, o barco que opere sobre alta mar debe estar regido por alguna jurisdicción nacional.

Utilización: La analogía de alta mar se usa para apoyar varias opiniones. A veces, se utiliza para justificar la necesidad de regular la Internet internacionalmente. En concreto, esta analogía sugiere el uso del antiguo derecho romano de *res communis omnium* (es decir, un espacio que sea parte de un patrimonio de la humanidad, que sea regulado y cosechado por todas las naciones) en Internet tal y como se usa en la regulación de alta mar. En otros casos, la analogía de alta mar se usa como argumento contra la regulación nacional de la Internet, ya que se la ve como un espacio que va más allá de la jurisdicción de cualquier país, como en el caso de la Antártida y el espacio exterior, junto con el de alta mar.

Clasificación de los asuntos de la gobernanza de Internet

La gobernanza de Internet es un área compleja, que requiere un mapeo conceptual inicial y clasificación. Su complejidad está relacionada con su naturaleza multidisciplinaria, que abarca una variedad de aspectos, como la tecnología, la socioeconomía, el desarrollo, el derecho, y la política.

La necesidad práctica de contar con una clasificación quedó claramente demostrada durante el proceso de la CMSI. En la primera fase, durante la etapa previa a la Cumbre de Ginebra (2003), muchos de los interesados, incluidos los estados nacionales, se encontraron con la dificultad de comprender la complejidad de la gobernanza de Internet. Un mapeo conceptual, brindado por las varias contribuciones académicas y el informe del GTGI, colaboró para lograr negociaciones más eficientes dentro del contexto del proceso de la CMSI. El informe del GTGI (2005) identificó cuatro áreas principales:

- Asuntos relacionados con la infraestructura y el manejo de los CIR.
- Asuntos relacionados con el uso de Internet, incluidos el correo no deseado, la seguridad de la red, y el cibercrimen.
- Asuntos de importancia para la Internet pero que tienen un impacto mucho más amplio que Internet y para los cuales existen organizaciones específicas que se encargan de ellos, como el derecho a la propiedad intelectual (IPR por sus siglas en inglés) o el comercio internacional.
- Asuntos relacionados con los aspectos del desarrollo de la gobernanza de Internet, en particular, la construcción de la capacidad de países en vías de desarrollo.

La agenda para el primer IGF, que se mantuvo en Atenas en 2006, fue elaborada sobre las siguientes áreas temáticas: acceso, seguridad, diversidad, y apertura. En el segundo IGF en Río de Janeiro en 2007, se agregó una quinta temática a la agenda: el manejo de los CIR. Estas cinco áreas temáticas influenciaron las agendas de todas las reuniones del IGF subsiguientes.

Aunque cambie la manera de clasificarlos, la gobernanza de Internet siempre aborda una misma serie de entre 40 y 50 asuntos específicos. Lo que varía es la relevancia de cada asunto en particular. Por ejemplo, mientras que el correo no deseado tuvo prominencia en la clasificación del GTGI en 2004, su relevancia política disminuyó en las reuniones de IGF, donde se convirtió en uno de los temas de menor prominencia dentro del área temática de la seguridad.

La clasificación de Diplo de la gobernanza de Internet agrupa los principales 40-50 asuntos en las siguientes siete canastas[30]:

- Infraestructura
- Seguridad
- Legal
- Económica
- De desarrollo
- Sociocultural
- De derechos humanos

Esta clasificación (Figura 4) refleja los enfoques políticos del GTGI y el IGF, así como también la investigación académica en este campo. La clasificación se desarrolló en 1997 y se ha modificado regularmente con base en los comentarios de los participantes en el curso (un

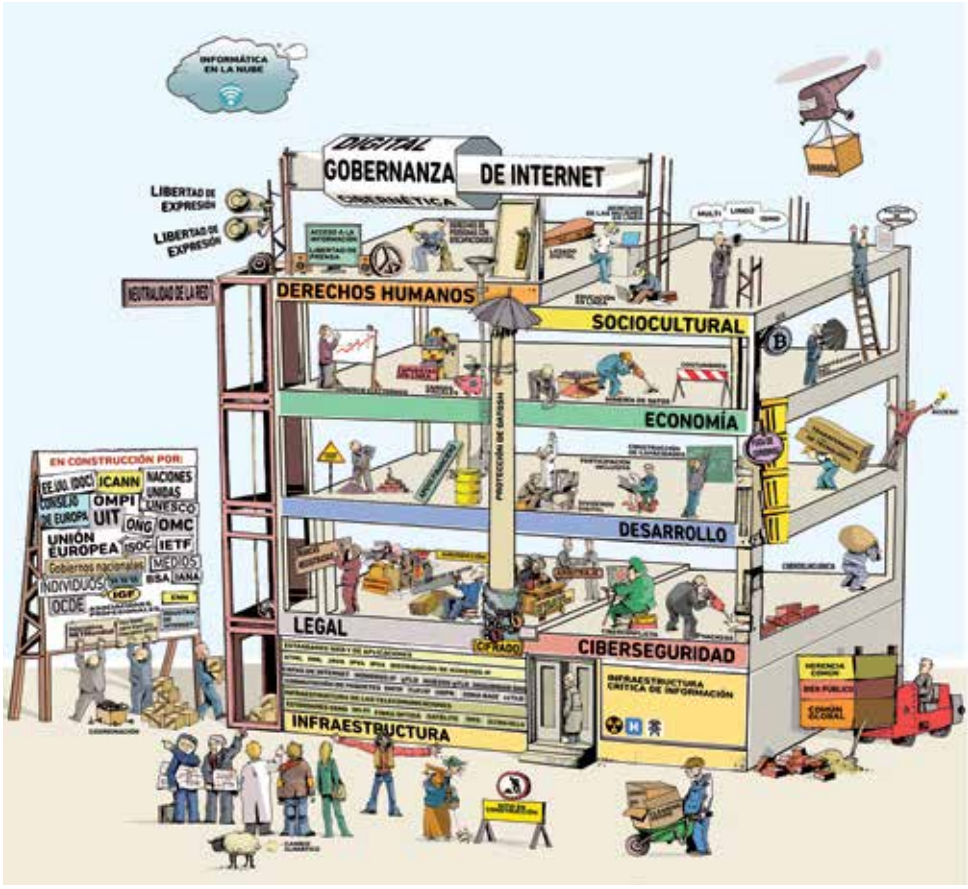

Figura 4. Edificio de la gobernanza de Internet en construcción

alumnado de más de 2000 personas a finales del 2015), resultados de búsqueda, percepciones desde el proceso de políticas, y la minería de datos. Una clasificación similar, basada en siete grupos, se usa en el informe *Mapa de los temas de políticas públicas de Internet* elaborado por la secretaría de la CSTD, para el panel de intersesiones de la Comisión de noviembre de 2014.[31]

Denominación, definición, y enmarcado de la gobernanza de Internet

Hemos debatido sobre las maneras alternativas para definir y enmarcar el concepto de la GI. El concepto sigue propenso a recibir diferentes interpretaciones, como se ilustra claramente en el edificio de la GI (Figura 4). En la cima del edificio, hay un cartel que dice «gobernanza de Internet» con una sección giratoria, que nos permite cambiar la frase «gobernanza *de Internet*» por «gobernanza *cibernética*» o «gobernanza *digital*». En el debate público sobre políticas, también se utilizan otros términos, como «políticas de Internet», «políticas digitales», y «diplomacia cibernética».

Este debate se complica aún más cuando incluimos la cuestión del alcance de la GI. Algunos afirman que, por ejemplo, la ciberseguridad es parte de la GI. Otros lo niegan, y toman a la ciberseguridad como un campo por separado. Hay quienes dicen que la GI tiene que ver exclusivamente con temas relacionados con ICANN (gestión de los nombres de dominio, direcciones IP, etc.). Otros extienden el alcance de la GI hacia una amplia serie de temas de políticas públicas relativas a la Internet.

Este debate no solamente posee una relevancia teórica. También tiene un impacto en los aspectos prácticos relativos a dónde, cómo y quién lleva a cabo y aborda los temas de políticas de Internet. Cuando se trata de términos y definiciones, no existe una solución simple para este debate. Las diferencias seguirán estando allí y resulta poco probable que nos pongamos de acuerdo sobre los términos y definiciones «correctos».

En este libro, utilizamos el término «gobernanza de Internet» de manera general; cubre más de 40 asuntos de políticas públicas de Internet, agrupados en 7 canastas. Este enfoque se basa en la definición de GI proporcionada por el GTGI, y la manera en que el término se utiliza en los procesos de la CMSI, en publicaciones, y en el ámbito de la investigación académica. El uso de diferentes términos y definiciones proviene de otras justificaciones de políticas e investigación.

Si bien no es muy probable que el debate acerca del término o la definición «correctos» sea particularmente efectivo o útil, es de gran relevancia tener un claro entendimiento sobre qué temas exactamente entran en cada término. Por ejemplo, ¿qué temas se debaten bajo los conceptos de GI, políticas digitales, o gobernanza cibernética? ¿Incluyen la ciberseguridad, el comercio electrónico, o la privacidad en línea, entre otros de los asuntos de políticas públicas de Internet? Comprender el alcance de cada término representa el primer paso para reducir la confusión e incrementar la claridad de los procesos de políticas.

Tarde o temprano, con a la perfecta integración de las herramientas digitales en la sociedad moderna, el debate sobre la terminología se hará menos relevante. El comercio electrónico se posicionará como una parte indispensable del comercio. La ciberseguridad continuará alineándose y apoyando las prioridades generales de la seguridad. Mientras más los avances digitales se hagan una parte intrínseca de nuestras vidas cotidianas, más probable será que la GI se funda con la gobernanza subyacente de la sociedad.

NOTAS FINALES

[1] La Resolución 56/183 de la Asamblea General de la ONU (del 21 de diciembre de 2001) respaldó la celebración de la Cumbre Mundial de la Sociedad de la Información (CMSI) en dos fases. La primera fase tuvo lugar en Ginebra del 10 al 12 de diciembre de 2003, y la segunda se celebró en Túnez, del 16 al 18 de noviembre de 2005. El objetivo de la primera fase fue desarrollar y fomentar una clara declaración de voluntad política y llevar a cabo los pasos necesarios para establecer los cimientos para una sociedad de la información para todos, que refleje todos los distintos intereses en juego. Más de 19000 participantes provenientes de 174 países asistieron a la cumbre y a eventos relacionados. Fuente: http://www.itu.int/net/wsis/basic/about.html [accedido el 28 de septiembre de 2016].

[2] La definición de GTGI sigue el patrón de las definiciones utilizadas frecuentemente en la teoría de régimen. El fundador de la teoría de régimen, Stephen D. Krasner, señala: *Los regímenes pueden ser definidos como un conjunto de principios implícitos o explícitos, normas, reglas y procedimientos de decisiones alrededor del cual las expectativas de los actores convergen en una determinada área de las relaciones internacionales. Los principios son creencias de hecho, causación y rectitud. Las normas son estándares de comportamiento definidos en términos de derechos y obligaciones. Las reglas son prescripciones o proscripciones específicas para la acción. Los procedimientos de toma de decisión son prácticas prevalecientes para la realización e implementación de las elecciones colectivas.* Krasner S (1983) Introducción, en *Regímenes Internacionales.* Krasner SD (ed.), Cornell University Press: Ithaca, NY, EE. UU.

[3] Shannon V (2006) What's in an 'i'? *International Herald Tribune,* 3 de diciembre de 2006. Disponible en: http://www.nytimes.com/2006/12/03/technology/03iht-btitu.3755510.html [accedido el 28 de septiembre de 2016].

[4] Barlow JP (1996) Declaración de independencia del ciberespacio. Disponible en https://www.eff.org/cyberspace-independence [accedido el 28 de septiembre de 2016].

[5] Para ver la evolución del uso de la palabra «Internet» durante la preparación de la Cumbre Mundial de la Sociedad de Información, consulte *The Emerging Language of ICT Diplomacy – Key Words* de DiploFoundation (2003). Disponible en https://www.diplomacy.edu/IGFlanguage/2004research [accedido el 3 de agosto de 2014].

[6] Informe del Grupo de Trabajo sobre la Gobernanza de Internet (2005). Disponible en http://www.wgig.org/docs/WGIGREPORT.pdf [accedido el 10 de octubre de 2016].

[7] La Agenda de Túnez de la Cumbre Mundial de la Sociedad de la Información (2005) para la Sociedad de la Información. Disponible en http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html [accedido el 10 de octubre de 2016].

[8] En junio de 2010, ICANN aprobó el dominio de nivel superior .xxx para el contenido para adultos.

[9] Para más información sobre la neutralidad de la red, vea nuestro video explicativo en https://www.youtube.com/watch?v=R-uMbZFfJVU [accedido el 3 de octubre de 2016].

[10] Clinton H (2010) Comentarios sobre la libertad de expresión. Disponible en http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm [accedido el 3 de octubre de 2016].

[11] Refiérase al párrafo 123 de la Agenda de Acción de Adis Ababa, adoptada en la Tercera Conferencia Internacional sobre la Financiación para el Desarrollo, que tuvo lugar entre el 13 y el 16 de julio de 2015. Disponible en http://www.un.org/esa/ffd/wp-content/uploads/2015/08/AAAA_Outcome.pdf [accedido el 10 de octubre de 2016].

[12] Banco Mundial (2016) Informe sobre el Desarrollo Mundial 2016: Digital Dividends. Disponible en http://www.worldbank.org/en/publication/wdr2016 [accedido el 3 de octubre de 2016].

[13] Drake W, Cerf V, Kleinwachter W (2016) Internet Fragmentation: An Overview. Disponible en http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf [accedido el 3 de octubre de 2016].

[14] Comisión Global sobre la Gobernanza de Internet (2016) One Internet. Disponible en https://www.ourinternet.org/report [accedido el 3 de octubre de 2016].

[15] Wiener N (1948) *Cibernética: O el control y comunicación en animales y máquinas*. París: Hermann & Cie, Cambridge, MA: Technology Press, y Nueva York: John Wiley & Son.

[16] Gibson W (1984) *Neuromancer*. Nueva York: Ace Books.

[17] Newitz A (2013) The bizarre evolution of the word 'cyber'. Disponible en http://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487 [accedido el 3 de octubre de 2016].

[18] Comisión Europea (2015) Una Estrategia de Mercado Único Digital para Europa. Disponible en http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX%3A52015DC0192 [accedido el 11 de octubre de 2016].

[19] Citado en Helfand D (2001) Edpseak is in a class by itself. *Los Angeles Times*, 16 de agosto. Disponible en http://articles.latimes.com/2001/aug/16/news/mn-34814 [accedido el 3 de octubre de 2016].

[20] Esta sección no podría haber estado completa sin el debate con Aldo Matteucci, asociado principal de Diplo, cuyas opiniones inconformistas sobre las cuestiones de la gobernanza moderna representan una dosis de realidad en las actividades de enseñanza e investigación de Diplo.

[21] Asamblea General de la ONU (2015) Documento de Resultados de la Reunión de Alto Nivel de la Asamblea General sobre la revisión total de la implementación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información (Resolución A/70/L.33). Disponible en http://workspace.unpan.org/sites/Internet/Documents/UNPAN95735.pdf [accedido el 10 de octubre de 2016].

[22] OTAN (2016) Comunicado de la Cumbre de Varsovia. Disponible en http://www.nato.int/cps/en/natohq/official_texts_133169.htm [accedido el 10 de octubre de 2016].

[23] Broeders D (2015) *The public core of the Internet*. Amsterdam: Amsterdam University Press. Disponible en http://www.wrr.nl/fileadmin/en/publicaties/PDF-Rapporten/The_public_core_of_the_internet_Web.pdf [accedido el 3 de octubre de 2016].

[24] Vea la declaración del embajador Trigona durante la reunión de la Asamblea General de la ONU dedicada al Proceso de Revisión de la Cumbre Mundial sobre la Sociedad de la Información, del 15 de diciembre de 2015, en Nueva York: https://www.gov.mt/en/Government/Press%20Releases/Documents/pr152897a.pdf [accedido el 3 de octubre de 2016].

[25] El proceso de la CMSI empezó con la primera reunión preparatoria que se mantuvo en Ginebra en julio de 2002. La primera Cumbre se celebró en Ginebra (diciembre de 2003) y la segunda, en Túnez (noviembre de 2005).

[26] Volker Kitz brindó un argumento a favor de la analogía entre la administración de los sistemas de telefonía y nombres y números de la Internet. Kitz V (2004) *ICANN may be the only game in town, but Marina del Rey isn't the only town on Earth: Some thoughts on the so-called uniqueness of the Internet*. Disponible en: http://studentorgs.law.smu.edu/Science-and-Technology-Law-Review/Articles/Fall-2005/Kitz.aspx [accedido el 3 de octubre de 2016].

[27] Corte Suprema de EE. UU. (1997) Fallo sobre Reno vs la Unión Estadounidense por las Libertades Civiles. Disponible en https://supreme.justia.com/cases/federal/us/521/844/case.html [accedido el 10 de octubre de 2016]

[28] Citado en Mock K, Armony L (1998) *Hate on the Internet*. Disponible en http://archive.is/M70XS [accedido el 3 de octubre de 2016].

[29] Fragmentos del discurso del Secretario General de la UIT, pronunciado en la reunión de ICANN en el Cairo (6 de noviembre de 2008). Disponible en: https://cai.icann.org/files/meetings/cairo2008/toure-speech-06nov08.txt [accedido el 3 de octubre de 2016].

[30] El término « canasta » se introdujo en la práctica diplomática durante las negociaciones de la Organización para la Seguridad y la Cooperación en Europa (OSCE).

[31] CSTD (2015) Mapa de los temas de políticas públicas de Internet. Disponible en http://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2_en.pdf [Accedido el 19 de octubre de 2016]

Sección 2

LA CANASTA DE INFRAESTRUCTURA

La canasta de infraestructura

La canasta de infraestructura incluye los asuntos básicos, más que nada técnicos, relacionados con el funcionamiento de Internet. El criterio principal para añadir un tema en esta canasta es su relevancia en la funcionalidad básica de Internet. La canasta incluye los elementos esenciales, sin los cuales no existiría la Internet ni la World Wide Web (www)[1]. Estos temas están agrupados en tres grandes áreas que, hasta cierto punto, siguen el modelo de tres capas de Internet que muestra la Figura 5:

1. La infraestructura de telecomunicaciones, por la cual fluye todo el tráfico de Internet

2. Los asuntos técnicos relacionados con los estándares (estándares web y técnicos) y los recursos críticos de Internet (números de Protocolo de Internet, el Sistema de Nombres de Dominio, y la zona raíz).

3. Los asuntos transversales en los que se encuentran la neutralidad de la red, la computación en la nube, la Internet de las Cosas (IoT, por sus siglas en inglés), y la convergencia.

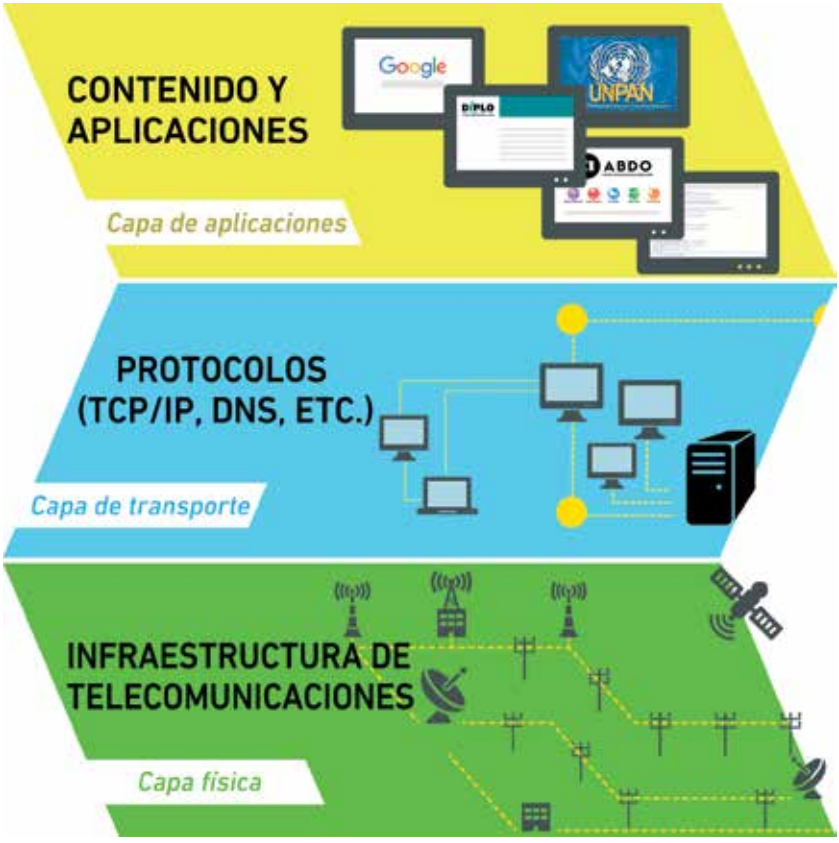

Figura 5. Capas de Internet

La infraestructura de telecomunicaciones[2]

La situación actual

La Internet utiliza la infraestructura de telecomunicaciones como el medio por el cual fluye el tráfico: el cableado como los cables de cobre y la fibra óptica; las ondas electromagnéticas como los satélites, enlaces inalámbricos, y redes móviles. En muchos casos, la infraestructura de telecomunicaciones existente – como las líneas telefónicas, la conectividad móvil, la red eléctrica[3], los cables submarinos, o los enlaces satelitales – se utiliza para trasladar paquetes de Internet. Progresivamente, se está empleando una infraestructura de telecomunicaciones innovadora para transportar datos – como el cableado submarino de fibra óptica de banda ancha, redes móviles de quinta generación (5G), y soluciones inalámbricas novedosas como los globos de Google[4] o los Espacios en Blanco de Televisión,[5] así como también tecnologías que habilitan el mejor empleo de la IoT.

Las tecnologías de conectividad de Internet más comúnmente utilizadas

Infraestructura de telecomunicaciones cableada

- Líneas de Suscripción Digital (DSL, por sus siglas en inglés): usan los cables de cobre telefónicos existentes para transmitir datos y tráfico de voz.
- Redes de televisión por cable: los servicios de cable de banda ancha brindan acceso a Internet sobre la infraestructura de televisión por cable.
- Fibra óptica: las redes de fibra óptica son la infraestructura troncal preferida de Internet, debido a que una sola fibra puede cargar con cantidades importantes de datos por largas distancias, sin deterioro significativo de señal por la distancia.
- Internet sobre líneas eléctricas: permite a los usuarios enchufar un dispositivo a una toma eléctrica e instantáneamente obtener un servicio de Internet de alta velocidad.

Infraestructura de telecomunicaciones inalámbrica

- Internet satelital: se usa para facilitar conectividad a Internet a comunidades en lugares en los que el acceso a Internet terrestre no se encuentra disponible, y a comunidades que se desplazan frecuentemente.
- Wi-Fi: permite que los dispositivos se conecten a redes de área local inalámbricas (WLAN, por sus siglas en inglés) mediante radiofrecuencias.
- WiMAX (Interoperabilidad para el Acceso a Microondas): facilita la entrega de acceso de banda ancha inalámbrico a largas distancias, como alternativa al cableado y a las DSL, mediante el uso de frecuencias licenciadas y no licenciadas.
- Banda ancha móvil: una de las tecnologías más usadas es el Sistema Global para las Comunicaciones Móviles (GSM, por sus siglas en inglés), que emergió en Europa y se está volviendo dominante a nivel global con su tercera y cuarta generación (3G y 4G), y, en un futuro, con la quinta generación.

La manera en la que se regulan las telecomunicaciones tiene un impacto directo sobre la gobernanza de Internet. La infraestructura de telecomunicaciones se regula tanto a nivel nacional como internacional. Las organizaciones internacionales clave vinculadas con la regulación de las telecomunicaciones incluyen a la UIT, que elaboró reglas para la coordinación entre los sistemas de telecomunicaciones nacionales, la distribución del espectro radioeléctrico, y la gestión del posicionamiento de satélites; y la Organización Mundial del Comercio (OMC), que ha cumplido un papel esencial en la liberalización de los mercados de telecomunicación en todo el mundo.[6]

Two Reglamentos de Telecomunicaciones Internacionales de la UIT

Los RTI de la UIT de 1988 facilitaron la liberalización internacional de los precios y servicios, y permitió un uso más novedoso de los servicios básicos, como el arrendamiento de líneas internacionales, en el campo de Internet. Brindaron una de las bases infraestructurales para el rápido crecimiento de Internet en la década de 1990. El RTI fue modificado en diciembre de 2012 durante la CMTI-12 en Dubái; 89 estados – más que nada países en vías de desarrollo – firmaron la modificación del RTI, mientras que otros 55 estados no lo hicieron, entre los que se encuentra EE. UU. junto con muchos estados europeos.[7] Por lo tanto, a partir del 1 de enero de 2015, cuando el RTI de 2012 entró en vigencia, dos regímenes de telecomunicaciones internacionales han estado en funcionamiento (1988 y 2012). Afortunadamente, debido a que las modificaciones de 2012 no fueron sustantivas, no afectaron la funcionalidad integrada del sistema de telecomunicaciones global. Aun así, esta «gobernanza dual» necesita solución.

Los roles que desempeñan la UIT y la OMC son bastante diferentes. La UIT establece detallados estándares técnicos voluntarios y regulaciones internacionales específicamente para telecomunicaciones, y brinda asistencia a países en vías de desarrollo.[8] La mayoría de las controversias políticas están relacionadas con el abordaje, por parte de la UIT, de asuntos de políticas que están en el límite entre la infraestructura de las telecomunicaciones e Internet, como el VoIP, la ciberseguridad, y los identificadores de objetos digitales (Arquitectura de Identificación de Objetos Digitales – DOA).[9] La OMC brinda un marco para las normas generales del mercado.[10] Su rol en el campo de las telecomunicaciones no ha sido muy controvertido hasta ahora. Sin embargo, la incrementada participación activa de la OMC en el comercio electrónico puede impulsar un debate sobre los aspectos relacionados con el abordaje de zonas fronterizas entre el comercio electrónico y campos relativos a la ciberseguridad y la protección de datos.

Los asuntos

Los cables de la red troncal de Internet[11]

Desde que el primer cable telegráfico llegó a la India a través del Mar Mediterráneo, el Mar Rojo, y el Océano Índico, en la década de 1870, la mayor parte del tráfico de comunicaciones electrónicas internacionales fluye por medio de cables submarinos. Actualmente, más del 90% del tráfico de Internet global fluye a través de cables de fibra óptica submarinos, que siguen a gran medida las viejas rutas geográficas usadas por el telégrafo.

Los cables de Internet submarinos llegan a tierra en unos cuantos nodos de tráfico de Internet. La mayoría de los cables en América Latina llegan a tierra firme en Miami. En Asia, los nodos de tráfico de Internet clave son Singapur y Hong Kong. Otros puntos clave

para el tráfico de Internet son Ámsterdam, Nueva York, y San Francisco. El punto más vulnerable para los cables de Internet y para el tráfico continúan siendo los *hotspots* tradicionalmente estratégicos, incluidos los Estrechos de Luzón, Ormuz, y Malaca, así como también el Canal de Suez.

La geografía también es importante en lo que respecta a la conectividad digital entre Asia y Europa. Por ejemplo, el 95% del tráfico de Internet entre Asia y Europa fluye a través de Egipto, de manera similar al transporte marítimo que usa el Canal de Suez como acceso directo.

Debido a que la mayor parte del tráfico de Internet fluye actualmente a través de cables submarinos, la instalación de nuevos cables de Internet terrestres es considerada, a menudo, un paso importante hacia la diversificación del tráfico de Internet, en especial entre Asia y Europa.

La Comisión Económica y Social de las Naciones Unidas para Asia y el Pacífico (UNESCAP) y el Banco Asiático de Desarrollo han estado promoviendo un componente digital de la red de autopistas asiáticas; un proyecto de infraestructura de transporte transcontinental que abarca 141.000 km.[12] Además, la Superautopista Transeuroasiática de la Información (TASIM, por sus siglas en inglés) planea conectar Europa Oriental con Asia Central, para obtener una mayor diversificación del flujo de datos entre los dos continentes. El objetivo del proyecto es «aumentar la velocidad de conexión con los socios de Asia Oriental y mejorar la resiliencia de Internet», y, en el proceso, también reforzar la cooperación regional en Asia Central.[13]

Los aspectos digitales también poseen un peso importante en la iniciativa «Un Cinturón, Una Ruta», que incluye el proyecto de la Ruta de Seda Digital.[14] La conexión digital podría beneficiarse de los proyectos infraestructurales de transporte y energía, que abarcarán la colocación de cables de fibra óptica a lo largo de vías férreas y conductos de energía.

Todos los proyectos previstos sobre los cables terrestres, y en particular la Ruta de la Seda Digital, podrían, por primera vez en la historia, desplazar un volumen considerable del tráfico de comunicaciones del lecho marítimo al cableado terrestre.

El bucle local – la última milla

El «bucle local» (o «la última milla») es el nombre que se le da a la conexión entre los Proveedores de Servicios de Internet (PSI) y sus clientes individuales. Los problemas con este bucle local (como las líneas de cableado en malas condiciones, los cortes de energía, etc.) representan un obstáculo para el uso extendido de Internet en muchos países, por lo general en vías de desarrollo. La comunicación inalámbrica es una posible solución de bajo costo para el problema del bucle local. En los últimos años, Google ha llevado a cabo experimentos para brindar acceso móvil inalámbrico desde globos (Proyecto Loon), mientras que Facebook ha estado trabajando para brindar acceso a Internet mediante el uso de una flota de drones. Además de las crecientes opciones tecnológicas disponibles, la solución al problema del bucle local también depende de la liberalización de este segmento del mercado de las telecomunicaciones, lo que también incluye permitir a múltiples operadores que usen la última milla de la red telefónica (conocido como el proceso de desagregación del bucle local).

La liberalización de los mercados de telecomunicaciones

Históricamente, la infraestructura y los servicios de telecomunicación provenían de operadoras estatales sobre la base de monopolios. Durante los últimos veinte años, muchos países han liberalizado sus sectores de telecomunicación e introducido competencia al mercado al permitir que nuevas operadoras entren al mercado y brinden redes y servicios

de comunicación electrónica de calidad competitiva. La liberalización también significó que los nuevos proveedores de servicios tenían permitido acceder a la infraestructura existente (que era propiedad del estado). La privatización de las operadoras de telecomunicaciones estatales ha traído aparejada la liberalización de las políticas. Sin embargo, este proceso se ha desplegado más lentamente en los países en vías de desarrollo. A menudo se enfrentan con el dilema, por un lado, de liberalizar el mercado de telecomunicaciones, lo que reduciría los costos de comunicación y propulsaría el desarrollo económico, y, por el otro, de preservar los monopolios de telecomunicaciones como fuentes de ganancias presupuestarias significantes (algo que pueden gozar especialmente gracias al sistema de acuerdos interempresariales internacionales de la telefonía tradicional). Tales consideraciones económicas llevaron al cuestionamiento sobre la redistribución de las ganancias provenientes de los servicios de comunicación de Internet, que fue propuesta por algunos países en vías de desarrollo en la CMTI-12 y otras reuniones internacionales.

El manejo del espectro electromagnético

Aunque generalmente se considere que la comunicación inalámbrica es una de las alternativas más convenientes en lo que concierne al empleo de una infraestructura cableada, uno de los inconvenientes del espectro es su escasez. En la teoría, se podría dividir cada segmento de frecuencia en pequeñas e infinitas partes, pero en la práctica el equipamiento que se utiliza – aunque está en constante mejora para una utilización del espectro más eficiente – tiene sus limitaciones en cuanto a la estrechez de las bandas de frecuencias que puede utilizar y aun así evitar interferencias de otros equipos con frecuencias similares. Esto sugiere que debería existir una autoridad encargada de designar frecuencias de banda específicas para el uso de uno o más tipos de servicios de comunicación radiales, y también para asignar los segmentos específicos del espectro para las operadoras específicas inalámbricas – estaciones de TV, emisoras de radio, operadoras de redes móviles, y los proveedores de servicios de Internet, entre otros.

La administración de la frecuencia en cada país (es decir, las decisiones sobre qué tecnologías y qué proveedores pueden utilizar determinados subsegmentos del espectro designado y bajo qué licencias) queda a menudo en manos de las autoridades que regulan las telecomunicaciones nacionales, y que unifican sus distribuciones locales con los países limítrofes y otros países de manera bilateral o mediante iniciativas regionales (como el Comité del Espectro Radioeléctrico [RSC] y el Grupo de Política del Espectro Radioeléctrico [RSPG]) o instituciones internacionales (como la UIT).

Por ejemplo, tanto en EE. UU. como en la mayoría de los estados miembros de la UE, la concesión de derechos del uso de frecuencias radioeléctricas se realiza a través de procesos de subastas públicas, en los que se presentan las frecuencias. La UE también ha desarrollado un enfoque regulatorio integral para el manejo del espectro radioeléctrico, con el objetivo de armonizar el uso de las frecuencias radioeléctricas entre los estados miembros.[15] El licenciamiento del uso de ciertas partes del espectro y la designación de estas a aquellos que puedan pagarlas en su mayor proporción – como las operadoras de redes móviles – asegura que el uso del espectro se dará en concordancia con ciertas necesidades, pero a su vez brinda ganancias significantes a los estados.

El desarrollo de nuevos servicios de comunicación que hacen uso del espectro radioeléctrico, en especial la banda ancha inalámbrica y las comunicaciones móviles, provocó un aumento en la demanda de radiofrecuencias, lo que instó a los gobiernos alrededor del mundo a buscar soluciones para acordar un uso óptimo del espectro. Una de las maneras de extender la banda del espectro utilizable para las comunicaciones digitales es liberar

grandes porciones del espectro que están ocupadas por las emisoras de TV análogas: motivando a las compañías emisoras a cambiar la señal análoga tradicional por una señal digital (lo que requiere una gran inversión en los nuevos equipos de emisión y nuevos dispositivos para cada hogar pero brinda una mejor calidad de servicio y la oportunidad de ofrecer otros servicios), se podría lograr que grandes cantidades del espectro queden libres para ser designadas a otros servicios – el denominado dividendo digital.

El volumen y los límites del uso del espectro se ven influenciados por los desarrollos tecnológicos. Esto disparó una discusión por parte de algunos grupos sobre que la regulación gubernamental actual debería ser remplazada por un «espectro abierto»; es decir, acceso abierto para todos, lo que seguiría al enfoque sin licenciamiento usado en el Wi-Fi normal (no existe una necesidad de licenciamiento para instalar una red Wi-Fi hogareña o de otro tipo). Sin embargo, existen dos posibles problemas con esta opinión. El primero está relacionado con la enorme inversión que realizaron las compañías de telecomunicaciones, especialmente en Europa, para adquirir el derecho de operar redes de teléfonos móviles 3G y 4G. Una política de espectro abierto sería injusta para estas empresas. Podría desencadenar sus quiebras e inestabilidad en el sector de las telecomunicaciones. El otro es que si el espectro se convierte en un recurso libre para todos, eso no significa necesariamente que será usado como un bien público, para el beneficio de muchos. Más bien, podría ser usado principalmente por actores que poseen las capacidades técnicas para aprovechar este espectro «libre» con el objetivo de conseguir sus propios intereses, inclusive para obtener ganancias.

Proveedores de acceso a Internet

La arquitectura de acceso a Internet está conformada por tres niveles: Los PSI que conectan a los usuarios finales constituyen el Nivel 3. Los Niveles 1 y 2 están conformados por los proveedores de ancho de banda de Internet (IBP, por sus siglas en inglés). Las empresas del Nivel 1 son los IBP más importantes. Usualmente, tienen acuerdos de intercambio de tráfico (*peering*)[16] con otros IBP del Nivel 1. La principal diferencia entre los IBP del Nivel 1 y 2 es que los del Nivel 1 intercambian tráfico a través del *peering*, mientras que los del Nivel 2 tienen que pagar aranceles de tránsito a los proveedores del Nivel 1.[17] El Nivel 1 por lo general está dirigido por grandes compañías, como AT&T, Verizon, Level 3 Communications, Vodafone, y NTT Communications.

Los asuntos

Los monopolios de las telecomunicaciones y los PSI

Es común en los países que poseen monopolios de telecomunicaciones que estos además provean acceso a Internet. Los monopolios impiden que otros PSI entren a este mercado, e inhiben la competencia. Eso resulta en precios más altos y a menudo en una menor calidad de servicio (QoS), y no consigue reducir el dividendo digital. En algunos casos, los monopolios de telecomunicaciones toleran la existencia de otros PSI, pero interfieren en su nivel operacional (por ejemplo, brindando anchos de banda más bajos o causando interrupciones en los servicios).

La liberalización de las telecomunicaciones y el rol de los PSI y los IBP

Existen opiniones encontradas sobre hasta qué punto los PSI y los IBP deberían estar sujetos a los instrumentos internacionales existentes. Uno de los puntos de vista, compartido

más que nada por los países desarrollados, afirma que las normas liberalizadas concedidas por la OMC a las operadoras de telecomunicaciones deberían extenderse a los PSI. Otros, mayoritariamente los países en vías desarrollo, señalan que el régimen de telecomunicaciones de la OMC corresponde únicamente al mercado de telecomunicaciones. Desde esta perspectiva, la regulación del mercado de los PSI exige nuevas normas por parte de la OMC.

El rol de los PSI en la aplicación de normas legales

Debido a que los PSI conectan a los usuarios finales con la Internet, se considera que tienen la capacidad de brindar la aplicación más exacta y directa de las normas legales sobre Internet. Por eso, muchos estados han comenzado a concentrar sus esfuerzos de aplicación de la ley en los PSI, en áreas como la violación del derecho de autor, la protección de los niños en línea, y otros campos relacionados con las políticas de contenido.

Consulte la Sección 4 para conocer más acerca del debate sobre el rol de los intermediarios.

¿Debería considerarse a la infraestructura de Internet como un servicio público?

Los datos de Internet pueden fluir sobre cualquier medio de telecomunicación. En la práctica, las instalaciones como las redes troncales del Nivel 1 (es decir, las principales rutas de datos entre redes grandes, estratégicamente interconectadas, y los enrutadores de núcleo en Internet), que usualmente cuentan con cables ópticos o enlaces satelitales, se han vuelto esenciales en el funcionamiento de Internet. Su papel primordial dentro de la red de Internet les concede a sus propietarios el poder de mercado necesario para imponer precios y condiciones para la prestación de sus servicios.[18] Básicamente, el funcionamiento de Internet podría depender de las decisiones que tomen los propietarios de las redes troncales centrales. La tendencia de los crecientes flujos de volumen de datos ha causado la aparición de nuevos actores en juego que originalmente no estaban conectados con el sector de las telecomunicaciones de manera directa. Por ejemplo, Google, Facebook y Microsoft han estado financiando la instalación de sus propios cables submarinos durante los últimos años.[19]

¿Se puede garantizar la fiabilidad de la Internet?

¿Es posible que la comunidad global de Internet solicite seguridades y garantías con respecto al funcionamiento fiable de la infraestructura crítica de Internet a las principales compañías de Internet y operadoras de telecomunicaciones? Actualmente, no existen tales disposiciones. Sin embargo, la tendencia en la discusión parece ser que lo que está en cuestión tiene que ver con la imposición de ciertos requisitos públicos sobre las operadoras privadas de la infraestructura de Internet.

Los IBP y la infraestructura crítica

A principios de 2008, se provocó una interrupción cuando uno de los principales cables de Internet se cortó en el Mar Mediterráneo cerca de Egipto. El incidente puso en peligro el acceso a Internet en una gran región que se extendía hasta la India. Dos incidentes

similares con cables de Internet cerca de Taiwán y Pakistán demostraron claramente que la infraestructura de Internet es parte de una infraestructura crítica nacional y global. La interrupción de los servicios de Internet puede afectar a la economía y la vida social de una región. La posibilidad de tal interrupción deja como resultado algunas preguntas:

- ¿Están protegidos adecuadamente los principales cables de Internet?
- ¿Cuáles son los respectivos roles de los gobiernos nacionales, las organizaciones internacionales, y las compañías privadas con respecto a la protección de los cables de Internet?
- ¿Cómo podemos manejar los riesgos asociados con la posible alteración de los cables de Internet?

www.igbook.info/infrastructure

Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP)

La situación actual

El TCP/IP es el principal estándar técnico de Internet. Se basa en tres principios:

- Conmutación de paquetes: los mensajes se dividen en pequeñas porciones llamadas «paquetes» y se envían de manera separada a través de distintas rutas en la Internet. Luego, se vuelven a ensamblar para formar el mensaje original en el punto de destino.

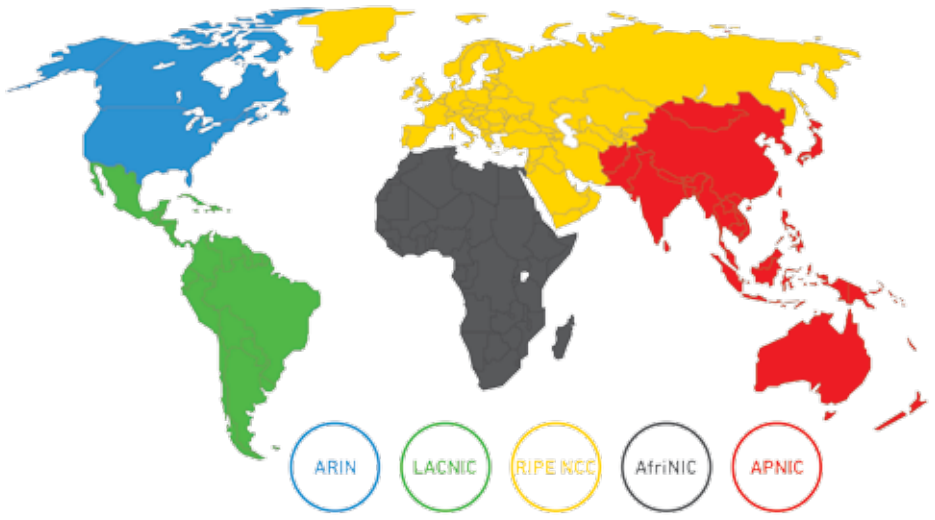

Figura 6. Registros Regionales de Internet

- Redes de extremo a extremo: uno de los principios de diseño centrales señala que las operaciones y servicios de las comunicaciones deberían tener lugar en los puntos de partida y de destino, mientras que la red debería ser tan neutral y «agnóstica» como sea posible.

- Robustez: el envío de datos debería ajustarse a las especificaciones, mientras que la recepción de datos debería ser más flexible, para que sea capaz de aceptar información que no se ajusta a las especificaciones.

Con respecto al protocolo TCP/IP, existen dos aspectos principales relacionados:

- La introducción de nuevos estándares.

- La distribución de números IP.

Los estándares TCP/IP están establecidos por IETF. Dado que estos estándares tienen una relevancia central para la Internet, la IETF los mantiene en constante y cuidadosa revisión. Cualquier cambio aplicable al protocolo TCP/IP exige un debate previo minucioso y la prueba segura de que tal cambio implicará una solución efectiva (por ejemplo, el principio de «el código que funcione».

Una dirección (o número) IP es una dirección numérica única que debe tener cada dispositivo conectado a Internet; cada dirección especifica cómo llegar a una ubicación de red mediante el sistema de enrutamiento de Internet. En términos generales, dos dispositivos conectados a Internet no pueden tener la misma dirección IP.

El sistema para la distribución de los números IP está organizado de manera jerárquica. En la cima se encuentra la IANA, cuyas funciones actualmente son desempeñadas por los Identificadores Técnicos Públicos (PTI, por sus siglas en ingles), una subsidiaria de ICANN.[20] Los PTI distribuyen los bloques de números IP a los cinco registros regionales de Internet (RIR) (Figura 6).[21] Los RIR distribuyen los números IP a los registros de Internet locales (LIR) y a los registros de Internet nacionales (NIR), que a cambio distribuyen los números IP a PSI, compañías e individuos más pequeños, que se encuentran por debajo en esta jerarquía.

Los asuntos

La limitación de los números IP y la transición al IPv6

El repositorio de números IP en Internet Protocol version 4 (IPv4), que se introdujo en 1983, contiene unos cuatro mil millones de números, que inicialmente parecían ser suficientes para satisfacer la demanda de direcciones. Sin embargo, en febrero de 2011, la IANA anunció que ya no tenía bloques disponibles del IPv4 para asignar los RIR.

El agotamiento de los números IPv4 se ha acelerado, en los últimos años, con la introducción de los dispositivos con acceso a Internet (como los teléfonos móviles, los dispositivos inteligentes, las consolas de juegos, y los aparatos domésticos) y el aumento de la conectividad a Internet en todo el mundo. Los desarrollos en el área de la IoT también llevaron a un incremento en la demanda de direcciones IP, ya que los dispositivos de la IoT necesitan direcciones IP para conectarse a Internet. La preocupación acerca de que los números IP podrían acabarse y que a la larga podrían inhibir un mayor desarrollo de Internet llevó a la comunidad técnica a tomar tres acciones importantes.

Figura 7. IPv4 a IPv6

- Racionalizar el uso del repositorio de números IP existente mediante la introducción de Traducción de Direcciones de Red (NAT, por sus siglas en inglés): una técnica que permite que las computadoras en una red privada (como aquellas que emplean las compañías y organizaciones) compartan una misma dirección IP al conectarse a Internet.

- Abordar el problema de los derrochadores algoritmos de designación de direcciones que se usaban previamente en los RIR mediante la introducción del Enrutamiento entre Dominios sin Clases (CIDR, por sus siglas en inglés): un esquema de direccionamiento IP que, con palabras sencillas, permita que una sola dirección IP designe muchas direcciones IP únicas (haciendo más eficaz la asignación de direcciones IP).

- Introducir una nueva versión del protocolo – *Internet Protocol version 6 (IPv6)* – que provea un repositorio de números IP (más de 340.000.000.000.000.000.000.000).

La comunidad técnica de Internet respondió proactivamente al problema de una posible escasez de números IP. Mientras que la NAT y el CIDR proporcionaron un arreglo rápido para este problema, una solución apropiada y a largo plazo fue la transición al IPv6.

Sin embargo, aunque el IPv6 se introdujo en 1996, su empleo ha sido lento, debido a la falta de conciencia acerca de la necesidad de realizar la transición, así como también la limitación de fondos para invertir en nuevos equipos en los países en vías de desarrollo (Figura 7). Los expertos han advertido que una transición lenta hacia el IPv6 podría resultar en la denominada fragmentación técnica de Internet, en la que dos Internets paralelas – una habilitada por el IPv4, y otra por el IPv6 – no podrían interactuar entre sí. Se destacó este punto, por ejemplo, en un informe publicado a principios de 2016 por el FEM,[22] según el cual solamente el 4% de la Internet estaba en ese momento prestando el uso del IPv6.

La tecnología de Internet permite que el IPv4 y el Ipv6 coexistan; la mayoría de las redes que usan el IPv6 admiten direcciones tanto del IPv4 como del IPv6. No obstante, para la transición sin contratiempos entre los dos protocolos, se necesita un conjunto de técnicas

para implementar mecanismos para el verdadero funcionamiento de Internet, la coexistencia, el fácil mapeo de direcciones, y la migración de servicio de nombres. Las especificaciones de la IETF para el IPv6 contienen estrategias, herramientas y mecanismos pertinentes para la transición.[23]

Además del problema de la transición, el marco de políticas para la distribución del IPv6 requerirá una distribución adecuada de los números IP, que necesita la introducción de mecanismos abiertos y competitivos para abordar las necesidades de los usuarios finales de la mejor manera posible. Incluso con la introducción del IPv6, podría surgir, de todas formas, una escasez «artificial», si los responsables de asignarlos a nivel local, como los PSI, eligen abusar de su poder y vincular dicha asignación a, por ejemplo, la adquisición de otros servicios, afectando así la disponibilidad y el precio de los números IP.

La transición del IPv4 al IPv6 requiere la participación de una amplia gama de partes interesadas. Las organizaciones técnicas como la IANA/PTI, los RIR, y la IETF necesitan asegurar una administración eficiente y efectiva de los recursos del IPv6, y desarrollar las especificaciones y los estándares necesarios para su uso. Los PSI deben implementar técnicas para garantizar la comunicación entre el IPv4 y el IPv6, e introducir a este último en sus redes y servicios. Los fabricantes de equipos (sistemas operativos, equipos de red, etc.) y desarrolladores de aplicaciones (*software* empresarial, tarjetas inteligentes, etc.) deben asegurarse de que sus productos y aplicaciones sean compatibles con el IPv6. Además, los proveedores de servicios de la sociedad de la información tienen que implementar el IPv6 en sus servidores.[24]

Cambios en el protocolo TCP/IP y la ciberseguridad

La seguridad no era uno de los temas más importantes para los primeros desarrolladores de la Internet Internet (en 1970-1980), ya que, en ese momento, la Internet solo consistía en una red cerrada de instituciones de investigación. Con la expansión de Internet a tres mil millones de usuarios en todo el mundo y su creciente importancia como infraestructura comercial y social, la cuestión de la seguridad es una de las primeras en la lista de asuntos de la gobernanza de Internet.

Si bien el IPv4 ofrece soporte técnico para seguridad IP (llamado IPSec), esta característica es opcional. En el IPv6 se necesita la seguridad y el IPSec es una parte integral que permite la autenticación, el cifrado, y la compresión del tráfico de Internet sin tener que adaptar ninguna aplicación.[25]

El IPv6 aborda las vulnerabilidades de seguridad que se sabe que afectan a la red del IPv4, que incluyen la autenticación de dispositivos, la integridad de los datos, y la confidencialidad. Aunque el IPv6 ofrece una mejor seguridad para estos casos, el protocolo también plantea nuevos problemas de seguridad a causa de la mala implementación y configuración, lo cual es más probable que con el protocolo IPv4, debido a su mayor simpleza.[26] Muchas de estas preocupaciones pueden ser mitigadas por cuidadosos procesos de transición, pero el miedo por estas preocupaciones, la falta de conciencia, y la prioridad secundaria hacen que, por ejemplo, muchas empresas retrasen la transición.[27]

Además, existen preocupaciones acerca de la posibilidad de que las direcciones del IPv6 perjudiquen la privacidad, ya que cada dispositivo conectado tendrá asignado un identificador único. No es necesario, sin embargo, que este identificador permanezca estático, pero podría asignarse de manera dinámica y cambiar ocasionalmente; por lo tanto, la manera en que se implemente el IPv6 será importante para este aspecto.

Cambios en el protocolo TCP/IP y el problema de la limitación del ancho de banda

Para facilitar la entrega de contenido multimedia (por ejemplo, la telefonía en Internet, o vídeo por demanda) es necesario brindar una calidad de servicio (QoS) capaz de garantizar un nivel mínimo de desempeño. La QoS es particularmente importante en las aplicaciones sensibles a las demoras, como la transmisión de eventos en vivo, y a menudo resulta difícil de lograr debido a las restricciones del ancho de banda. La introducción de la QoS podría significar cambios en el TCP/IP, incluso un potencial desafío para el principio de la neutralidad de la red.

Debido a la continua evolución de las tecnologías de red, y a los desafíos que mencionamos aquí, las organizaciones en la comunidad técnica han comenzado a investigar la posibilidad de desarrollar una siguiente generación de protocolos de Internet que podrían ser más adecuados para las realidades de un panorama técnico en constante evolución. A modo de ejemplo, a principios de 2016, el Instituto Europeo de Normas de Telecomunicaciones (ETSI) estableció un grupo de trabajo con el objetivo de «identificar los requisitos para la siguiente generación de protocolos y arquitecturas de red»; se espera que el grupo analice temas como: direccionamiento, seguridad y autenticación, requisitos de la IoT, requisitos de la distribución de vídeo y contenido, y requisitos del comercio electrónico.[28]

www.igbook.info/protocols

El Sistema de Nombres de Dominio

La situación actual

El DNS traduce los nombres de dominio de Internet (como google.com) – que es más fácil de recordar y de utilizar para las personas – a direcciones IP, utilizadas por las computadoras y otros dispositivos para identificar un cierto recurso de Internet (se presenta un esquema simplificado de este proceso en la Figura 8).

Desde el punto de vista infraestructural, el DNS consiste en servidores raíz, servidores de dominios de nivel superior (TLD), y una gran cantidad de servidores DNS ubicados alrededor del mundo.[29]

Un TLD es el nivel más alto en la jerarquía DNS de Internet. El DNS incluye dos tipos principales de dominios de nivel superior: Los dominios de nivel superior genéricos (gTLD) y los dominios de nivel superior con código de país (ccTLD). Los gTLD comprenden a los TLD tradicionales, como com, .info, .net, y .org, y también a los relativamente nuevos gTLD (que se introdujeron al comenzar el 2014) como .pub, .بازار (bazaar), .rentals, .ngo, o .游戏 (juego). Mientras que la mayoría de los gTLD tienen una política de registración abierta, que permite la registración de nombres por parte de cualquier individuo o entidad interesada, también existen los gTLD que están restringidos o reservados para grupos/sectores/comunidades específicos. Por ejemplo, .aero es de registración abierta solamente para la industria del transporte aéreo, mientras que .bank solamente puede ser usado por instituciones bancarias autorizadas. Los ccTLD son TLD de dos letras que designan países o territorios específicos (como .uk para el Reino Unido, .cn para China, y .br para Brasil).

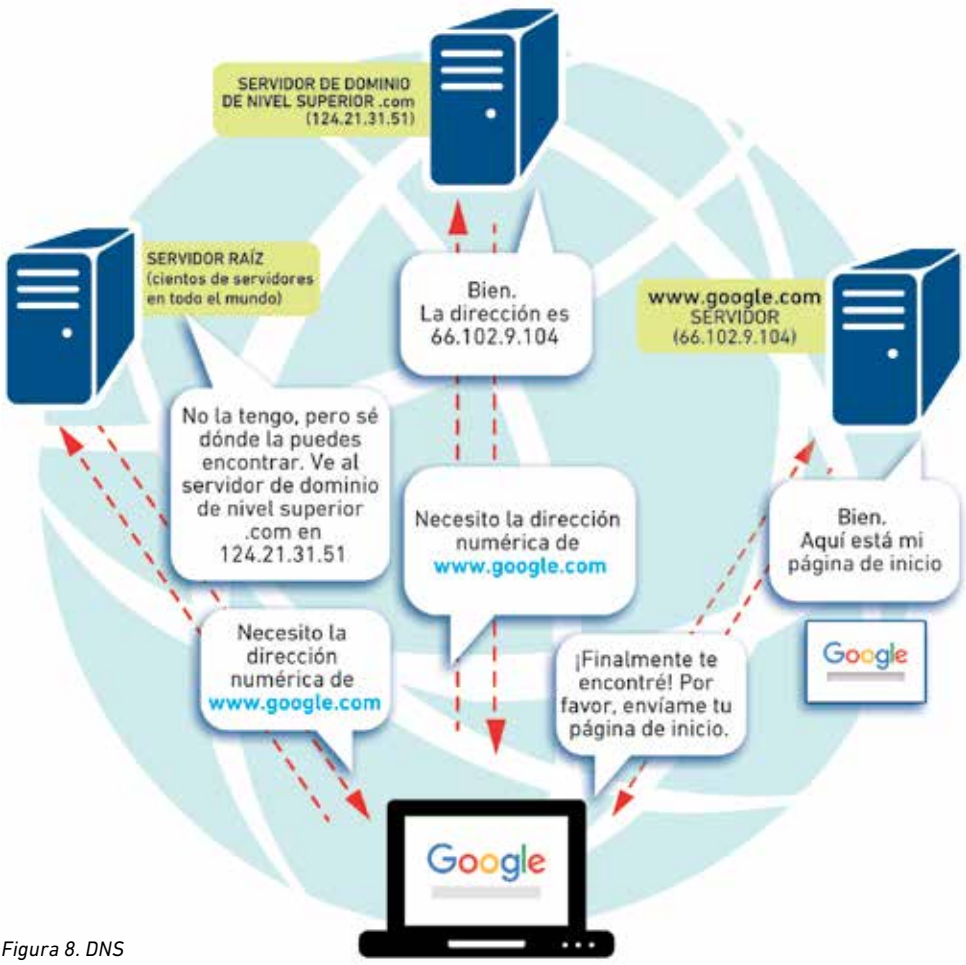

Figura 8. DNS

Todos los gTLD y ccTLD están administrados por un registro (también llamado operador de registro), cuya principal responsabilidad es mantener y administrar una base de datos con todos los nombres de dominios registrados en el respectivo TLD. Por ejemplo, el gTLD .com es administrado por VeriSign, mientras que a .uk lo administra Nominet. La registración de nombres de dominio, propiamente dicha, por los usuarios finales (llamados registrantes) se lleva a cabo mediante registradores. A pesar de que en la mayoría de los casos las funciones del registro y el registrador están claramente delimitadas, existen algunas excepciones: para algunos ccTLD, por ejemplo, el operador de registro puede también desempeñar la función del registrador.

ICANN asegura la coordinación general del DNS de la siguiente manera:

- Coordina la distribución y asignación de los nombres en el DNS de zona raíz.
- Coordina el desarrollo y la implementación de las políticas concernientes a la registración de nombres de dominio de segundo nivel en los gTLD.
- Facilita la coordinación del funcionamiento y la evolución del sistema de servidor de nombres raíz del DNS.[30]

Para los gTLD, ICANN celebra acuerdos con registros (para la administración de cada gTLD)[31] y acredita a los registradores.[32] Los ccTLD tienen una condición especial, en el sentido en que ICANN no establece reglas para administrarlos o gestionarlos. Existen, sin embargo, varios registros de ccTLD que celebraron algún tipo de acuerdo con ICANN (como los marcos para la rendición de cuentas, memorándums de entendimiento, e intercambio de correspondencia), principalmente con el propósito de establecer algunos principios de alto nivel para la relación entre las dos partes.

La coordinación operativa del DNS se lleva a cabo mediante la subsidiaria PTI de ICANN.

Consulte la Sección 9 para obtener más información sobre ICANN.

Los asuntos

Marcas comerciales

Un aspecto sensible relacionado con los nombres de dominio tiene que ver con la protección de marcas comerciales y los mecanismos de resolución de conflictos relacionados. El principio de «atención por orden de llegada» de la distribución de los nombres de dominio que se utilizaba en los primeros días de Internet impulsó un fenómeno conocido como «ciberocupación» (*cybersquatting*), la práctica de mala fe de la registración de nombres de dominio que representan a marcas comerciales registradas, generalmente con el propósito de revenderlos posteriormente a entidades que tienen derechos de marca sobre los nombres. La Política Uniforme para la Resolución de Controversias (URDP, por sus siglas en inglés), desarrollada por ICANN y la Organización Mundial de la Propiedad Intelectual (OMPI), brinda mecanismos que han reducido de manera significativa la ciberocupación.

Consulte la Sección 4 para obtener más información acerca de la propiedad intelectual.

La privacidad y la protección de datos

Otro elemento importante está asociado con la privacidad y la protección de datos en el contexto de los nombres de dominio. Actualmente, los registros mantienen bases de datos denominadas WHOIS, que contienen información sobre los nombres de dominios registrados, inclusive los datos de los registrantes. Con esta información (nombre, dirección de correo electrónico, dirección postal, etc.) a disponibilidad del público, surgieron preocupaciones, principalmente por parte de defensores de derechos civiles, quienes pidieron que se rediseñe la política del WHOIS. Varios debates sobre este asunto se han llevado a cabo dentro de ICANN en los últimos años, y ya está en marcha un proceso que tiene como objetivo rediseñar la política del WHOIS.

La creación de nuevos dominios de nivel superior genéricos

En 2012, tras seis años de asesoramiento y desarrollo de una nueva política, ICANN lanzó el Nuevo Programa gTLD, que amplió el DNS por encima de los 22 gTLD existentes en ese momento. Bajo este nuevo programa, cualquier organización del mundo podría postularse para dirigir un nuevo registro de gTLD, incluidas las escrituras no latinas, siempre y

cuando cumpla con una series de criterios establecidos en la Guía de Solicitantes de Nuevo gTLD. La introducción de nuevos gTLD fue recibida con entusiasmo por algunas partes interesadas, que vieron al programa como una oportunidad para mejorar la competencia y las opciones de elección del consumidor en el mercado de nombres de dominio. Otras preocupaciones que salieron a la luz, especialmente en relación con la protección de marcas comerciales en el contexto del creciente número de gTLD, y la potencial necesidad de que los titulares de las marcas lleven a cabo registraciones defensivas de nombres de dominios en múltiples gTLD, con el propósito de evitar la ciberocupación. Aunque el debate sobre la introducción de nuevos gTLD continúa, el programa está en funcionamiento; a finales de septiembre de 2016, había 1186 nuevos gTLD delegados (introducidos en el DNS).[33]

La propiedad intelectual no fue la única preocupación acerca de los nuevos gTLD. Los gobiernos representados en el Comité Asesor Gubernamental (GAC, por sus siglas en inglés) de ICANN centraron su atención en la necesidad de implementar medidas que aseguren la protección de los usuarios finales y preserven la competencia en el mercado en el contexto de la delegación de los nuevos gTLD. A modo de ejemplo, en el caso de los gTLD que representan sectores regulados (como .bank y .pharm), los gobiernos propusieron medidas para asegurar que solamente las entidades que posean las autorizaciones indicadas para operar en sus respectivos sectores puedan registrar nombres de dominio en dichos gTLD.

La protección de nombres e indicadores geográficos parece ser otro motivo de preocupación: ICANN frenó el proceso de delegación de .amazon para Amazon (vendedor en línea) luego de que los países latinoamericanos protestaron fuertemente dentro del GAC. La delegación de .wine/.vin se debatió acaloradamente dentro del GAC, en donde países como Suiza y Francia pedían medidas que previnieran la «registración abusiva» de los nombres de dominio que representaran nombres de vinos para los que existen indicaciones geográficas (en algunas jurisdicciones). Cuando ICANN asignó .africa a un grupo cuya aplicación fue apoyada por los países miembros de la Unión Africana, una compañía privada refutó la decisión.

La gestión de dominios de país

La gestión de los ccTLD comprende tres temas importantes. El primero tiene que ver con la decisión, a menudo políticamente controvertida, de qué países deberían ser registrados en lo que respecta a países y entidades que tienen un estado internacional poco claro o disputado (por ejemplo, los nuevos países independientes, los movimientos de resistencia). Un tema polémico fue la asignación de un nombre de dominio para la Autoridad Palestina.[34] En la justificación de la decisión de asignar el TLD .ps, la IANA reiteró el principio de asignar nombres de dominio de conformidad con el estándar ISO 3166 para los códigos de país, tal y como lo propuso Jon Postel, uno de los fundadores de Internet.

El segundo tema tiene que ver con quién debe gestionar los ccTLD. Actualmente, existen varios modelos de registros establecidos para los ccTLD.[35] En algunos casos, las funciones del registro son llevadas a cabo por una entidad pública (como una autoridad de regulación de telecomunicaciones nacional, un instituto de investigación dentro del gobierno, una universidad pública, etc.). También hay países en los que el gobierno establece reglas para la gestión del ccTLD, pero deja su real administración en manos del sector privado. En otros casos, son las compañías privadas las que se encargan de la administración de los ccTLD, sin participación por parte del gobierno. Además, existen varios registros ccTLD de múltiples partes interesadas, cuyas estructuras administrativas incluyen representantes de varios grupos de partes interesadas.[36]

Si, durante los primeros días de la Internet, parecía que los gobiernos mostraban desinterés por los ccTLD, la situación ha cambiado con el correr de los años, debido a que algunos gobiernos intentan obtener el control de sus dominios de país, a los que consideran recursos nacionales. Los gobiernos nacionales han elegido una amplia variedad de enfoques políticos.[37] La transición (redelegación) a una nueva institución que gestione el ccTLD (delegado) dentro de cada país es aprobada por ICANN bajo la condición de que no existan oposiciones por parte de las partes interesadas dentro del país.

El tercer tema tiene que ver con el hecho de que, a diferencia del caso de los gTLD, ICANN no impone reglas acerca de quién debería gestionar los ccTLDs, y acerca de cómo estos deberían gestionarse. ICANN solamente se limita a la delegación o redelegación de los ccTLD sobre la base de algunas guías de alto nivel que pretenden asegurar que el registro ccTLD sea técnicamente competente para gestionarlo, y que tenga el apoyo de la comunidad local para hacerlo.[38]

En 2005, el GAC de ICANN adoptó un conjunto de Principios y Lineamientos para la delegación y administración de dominios de nivel superior con códigos de país,[39] con la finalidad de que sirvan como guía para la relación entre gobiernos, los ccTLD, y ICANN. Uno de los principios centrales descriptos en este documento, que no es de carácter vinculante, es el de subsidiariedad, según el cual «la política ccTLD debería establecerse de manera local, a menos que se demuestre que el problema tiene un impacto global por lo que debe resolverse dentro del marco internacional».

Como se mencionó anteriormente, existen varios registros ccTLD que han celebrado algún tipo de acuerdo con ICANN, que establecieron principios de alto nivel para la relación entre ellos (los ejemplos incluyen Brasil, Chile, Países Bajos, Suecia, y el Reino Unido, entre otros). También hay muchos registros representados en la Organización de Apoyo para Nombres de Dominio con Código de País (ccNSO, por sus siglas en inglés) de ICANN, que desarrolla y recomienda políticas globales a la Junta de ICANN para un limitado conjunto de temas relacionados con los ccTLD (como la introducción de Nombres de Dominios Internacionalizados [IDN, por sus siglas en inglés]). Sin embargo, al mismo tiempo, algunos registros ccTLD se han mostrado reticentes a formar parte del sistema de ICANN (en septiembre de 2016, la ccNSO tenía 161 miembros, mientras que existían más de 240 ccTLD en ese momento).

Los operadores de dominios de país están organizados a nivel regional: Europa: Consejo Europeo de Registros Nacionales de Dominios de Nivel Superior (CENTR), África: Asociación Africana de Registros de Primer Nivel (AFTLD), Asia: Asociación de Asia Pacífico de Registros de Primer Nivel (APTLD), América Latina y el Caribe: Organización de ccTLD de América Latina y el Caribe (LACTLD).

Nombres de dominios internacionalizados

La Internet, en sus orígenes, era un medio de lengua inglesa. Gracias a su rápido crecimiento, se ha convertido en un espacio de comunicación global, que tiene un creciente número de usuarios no anglófonos. Durante mucho tiempo, la falta de funciones multilingües en la infraestructura de Internet fue una de las limitaciones más importantes para su desarrollo a futuro.

En mayo de 2010, tras un largo periodo de prueba e incertidumbres políticas, ICANN comenzó a aprobar los TLD en una amplia gama de escrituras, como el chino, arábico, y cirílico. Los IDN se introdujeron en varios países y territorios como equivalentes a sus

ccTLD latinos. Por ejemplo, en China, se introdujo 中国 además de .cn, mientras que en Rusia se introdujo рф aparte de .ru. Los IDN también son parte del Nuevo Programa gTLD, que permiten la registración de nuevos gTLD en escrituras diferentes de la latina; por ejemplo, .сайт (sitio web) y .онлайн (en línea) se encuentran entre los nuevos TLD disponibles al público.

La introducción de los IDN es considerada uno de los mayores éxitos del régimen de la gobernanza de Internet. Todavía existen, sin embargo, obstáculos técnicos, particularmente en lo que respecta a la habilitación de direcciones de correo electrónico utilizadas en cualquier escritura: aunque el TLD en las direcciones de correo electrónico ya puede ser un IDN, la parte inicial del correo (es decir, lo que antecede al símbolo «@») todavía debe escribirse usando la escritura latina. El reconocimiento de los IDN en los motores de búsqueda también sigue siendo un problema que necesita solución. Además de este problema técnico, que está siendo abordado por grupos dedicados de ICANN, queda el desafío de realmente generalizar el uso de los IDN; esto requiere crear conciencia acerca de esta posibilidad en países que no usan la escritura latina. La creación de servicios y contenidos también debería tomarse como una prioridad fundamental.

www.igbook.info/dns

Zona raíz y servidores raíz

Al estar en la cima de la estructura jerárquica del DNS, la zona raíz y los servidores raíz han llamado mucho la atención, en especial en los debates académicos y políticos sobre los temas de la gobernanza de Internet.

La situación actual

La función y la robustez del DNS pueden ilustrarse analizando la preocupación acerca de que la Internet colapsaría si se deshabilitaran los servidores raíz.

La zona raíz es el nivel más alto en la estructura técnica del DNS. El archivo de la zona raíz contiene las listas de los nombres y las direcciones IP de todos los TLD (tanto de los gTLD como de los ccTLD) en el DNS.[40] La gestión de la zona raíz es llevada a cabo por ITP, la subsidiaria de ICANN encargada de la operación de las funciones de la IANA. En el desempeño de sus funciones, los ITP asignan a los operadores de los TLD y mantienen una base de datos con sus datos técnicos y administrativos. El mantenimiento (actualización) del archivo de la zona raíz es llevado a cabo por VeriSign. Inicialmente, esta función de mantenimiento de la zona raíz era desempeñada sobre la base de un acuerdo de cooperación entre VeriSign y el gobierno de EE. UU., que, en el contexto de la transición de la administración de la IANA, fue remplazado por un acuerdo entre ICANN y VeriSign.

La zona raíz del DNS es operada por servidores raíz – también conocidos como servidores autoritativos, que guardan una copia pública del archivo de la zona raíz. Existe la confusión de que el número total de servidores raíz es 13. La realidad es que hay cientos de servidores raíz[41] esparcidos por varios sitios alrededor del mundo. El número 13 se origina en los 13 nombres de *host* diferentes,[42] debido a la limitación técnica del diseño del DNS. Doce entidades – instituciones públicas/ académicas (6), compañías comerciales (3),

e instituciones gubernamentales (3) – gestionan estas primeras instancias para garantizar que todos los servidores raíz dentro de la misma instancia tengan una copia actualizada del archivo de la zona raíz.

Si uno de los 13 nombres de *host* colapsa, los 12 restantes continúan en funcionamiento. Incluso en el caso de que los 13 se descompusieran simultáneamente, la resolución de nombres de dominio a las direcciones IP (función principal de los servidores raíz) continuaría gracias a otros servidores de nombres de dominio, distribuidos de manera jerárquica por todas partes de la Internet.

El sistema de servidores raíz se ve considerablemente fortalecido por el esquema Anycast,[43] que replica los servidores raíz por todas partes del mundo. Esto trae muchas ventajas, entre ellas una robustez aumentada del DNS y una resolución más rápida de las direcciones de Internet (con el esquema Anycast, los servidores que se encargan de la resolución se encuentran más cerca de los usuarios finales).

Por lo tanto, cientos de servidores de nombres de dominio cuentan con copias del archivo de la zona raíz. De esta manera no ocurriría un colapso inmediato y catastrófico en Internet. Pasaría algún tiempo hasta que se pudiese notar alguna consecuencia funcional grave, de modo que sería posible reactivar los servidores originales o crear nuevos servidores antes de que llegase ese momento.

Como se mencionó anteriormente, VeriSign se encarga de mantener y actualizar el archivo de la zona raíz. Por ejemplo, cuando ICANN aprueba un nuevo gTLD, esta información le llega a VeriSign, que realiza los cambios necesarios en la zona raíz (introduce el nuevo gTLD en la raíz) y distribuye el archivo de la zona raíz modificado a los servidores de nombre raíz.

Los asuntos

Raíces alternativas: viabilidad y riesgos

Uno podría preguntarse por qué ICANN tendría el derecho exclusivo de dictar la lista de los TLD y la manera en que estos se resuelven a direcciones IP – ¿Sería posible que no existan alternativas al sistema DNS? Mientras que ICANN – mediante los ITP, operadores de las funciones de la IANA – opera y administra la raíz oficial del DNS que utiliza la mayoría de los usuarios de la Internet pública para resolver nombres de dominio a direcciones IP, muchas organizaciones operan raíces activas alternativas del DNS (Raíces Alt). Aunque estas organizaciones ofrecen su propia variedad de TLD – que usualmente difieren bastante de la lista TLD de ICANN – , los usuarios finales que quieren hacer uso de tal servicio deben reconfigurar sus ajustes de red para desviarse de la raíz universal hacia la raíz alternativa. Una de las primeras raíces Alt es la AlterNIC que fue fundada en 1995, y se mantuvo en funcionamiento hasta la formación de ICANN en 1998.

Open NIC, New.net, y Name.space llevaron a cabo varios intentos por crear un DNS alternativo. La mayoría de esos intentos no tuvo éxito, ya que contaron solamente con un bajo porcentaje de usuarios de Internet.

Actualmente, existen varios servidores DNS alternativos que se encuentran en funcionamiento, incluidos el DNS Google, Open DNS, DNS Advantage, y ScrubIT.[44]

Otro proyecto relativamente nuevo y más ambicioso – el Proyecto DNS Yeti, lanzado en 2015 – planea «construir un sistema de raíz DNS del IPv6 experimental paralelo para descubrir los límites del servicio de nombres raíz del DNS».[45]

Crear un sistema alternativo de servidores de nombre raíz es técnicamente simple. La pregunta principal que hay que hacer es con cuántos seguidores contaría un sistema alternativo, o más específicamente, cuántas computadoras en Internet apuntarían a los servidores alternativos al momento de resolver los nombres de dominio. Sin usuarios, cualquier DNS alternativo sería inútil.

Discusión conceptual: sistema de servidores de raíz único vs alternativo

Durante mucho tiempo, el principio de un único sistema de servidores de nombre raíz era considerado como uno de los mantras principales de Internet, de los que se suponía que no se debía hablar y menos, modificar. Se presentaron muchos argumentos para evitar cualquier discusión que tuviera que ver con alternativas al sistema único. Uno de esos argumentos es que el sistema actual previene el riesgo de que el gobierno use el DNS para censurar. Sin embargo, el argumento de la censura en contra de los cambios en la política del DNS está perdiendo peso en el sentido funcional. Los gobiernos no necesitan tener control alguno del sistema DNS o del archivo de la zona raíz para llevar a cabo la censura. Podrían acudir a herramientas más efectivas, que se ocupen de filtrar el tráfico web.

Un argumento más sólido es que cualquier sistema raíz alternativo podría resultar en la fragmentación, e incluso quizás, en la desintegración total de Internet. Aunque todos los sistemas raíz usan el mismo sistema de números IP, utilizan distintos enfoques de denominación y diferentes técnicas de resolución. Puede ocurrir que varios sistemas raíz tengan el mismo nombre de dominio, pero cada uno lo resuelve a una dirección IP distinta. Sin embargo, debido a que la mayoría de las raíces DNS alternativas no son interoperables – ya sea con la raíz DNS de ICANN o entre ellas mismas – su coexistencia quiebra el principio universal de resolubilidad, que garantiza que exista una sola manera de resolver un TLD a una dirección IP – a menos que las raíces alternativas sean usadas con propósitos estrictamente privados, y no de manera pública. Desde una perspectiva del DNS, esto evita que algunas partes de la Internet alcancen otras partes. La fragmentación de Internet podría poner en peligro una de sus funciones centrales – la de servir como un sistema de comunicación global unificado. Cuán realista es este peligro?[46]

www.igbook.info/root

Neutralidad de la red

La clave del éxito de Internet yace en su diseño, que está basado en el principio de la neutralidad de la red. Desde un principio, el flujo de todo el contenido en Internet, ya sea proveniente de *start-ups* o de grandes compañías, recibió un trato sin discriminación. Las nuevas compañías e innovadores no necesitaban permiso ni poder de mercado para innovar en Internet. Con el crecimiento del uso y el desarrollo de servicios digitales nuevos, especialmente de los que consumen ancho de banda como la transmisión de vídeos de alta calidad, algunos operadores de Internet (compañías de telecomunicaciones y los PSI) comenzaron a priorizar un tráfico determinado – como sus propios servicios o los

servicios de empresas asociadas – basado en las necesidades y planes empresariales, justificando ese enfoque con la necesidad de recaudar fondos para invertirlos en la mejora de la red. Por otra parte, los defensores de la neutralidad de la red luchan fuertemente contra dichos planes, y argumentan que esto podría limitar el acceso abierto a la información y las libertades en línea, así como también estancar la innovación en línea.

La importancia de la neutralidad de la red para el éxito de Internet es clave. El debate acerca de mantener el principio de la neutralidad de la red atrajo a una amplia gama de actores, desde el presidente de EE. UU., Barack Obama, hasta los activistas de organizaciones de base de derechos humanos. La manera en la que se trate la neutralidad de la red puede impactar en el desarrollo futuro de Internet.

La situación actual

Tenemos que hacer una distinción entre la neutralidad de la red y la gestión del tráfico de red. Desde los primeros días de la conexión de módem de acceso telefónico a Internet, la gestión del tráfico de red se ha utilizado para hacer frente a una brecha entre el ancho de banda disponible y las necesidades de ancho de banda de los usuarios.Para poder enfrentar este desafío y brindar una buena calidad de servicio, los operadores de Internet (las compañías de telecomunicaciones y los PSI) – también conocidos como «prestadoras» – han utilizado varias técnicas de gestión del tráfico para priorizar un tráfico determinado. Por ejemplo, el tráfico de Internet que transmite conversaciones de voz mediante los servicios del VoIP (por ejemplo, Skype) deberían tener prioridad con respecto al tráfico que transmite un simple correo electrónico: aunque podemos notar desfasajes en las conversaciones por Skype, nunca notaremos los retrasos mínimos en un intercambio de correos electrónicos.

La necesidad de gestionar el tráfico es especialmente importante hoy en día, con las extensas demandas de altos anchos de banda: cada vez más usuarios usan Internet de manera regular para realizar llamadas de audio o vídeo (Skype, Google Hangout, teleconferencias), para jugar en línea, o para ver programas de TV y películas en una calidad de alta definición (HD), como por ejemplo, los servicios de Hulu o Netflix. La gestión del tráfico es importante para la comunicación inalámbrica debido a, por un lado, la expansión del uso de dispositivos móviles, y por el otro, las limitaciones técnicas del espectro inalámbrico.[47] La gestión del tráfico se está volviendo cada vez más sofisticada en lo que respecta al enrutamiento del tráfico de Internet de la manera más adecuada para brindar una buena calidad de servicio, evitando la congestión, y eliminando la latencia y el retardo por fluctuación.

La primera discordancia en la interpretación del principio de neutralidad de la red tuvo que ver con la posibilidad de que la gestión del tráfico quede completamente prohibida. Los puristas de la neutralidad de la red afirmaron que «todos los bits se crean iguales» y que todo el tráfico de Internet debería recibir el mismo trato. Las empresas de telecomunicaciones y los PSI se opusieron a este punto de vista argumentando que son los usuarios los que deben recibir un acceso equitativo a los servicios de Internet y que para que esto suceda, no todo el tráfico de Internet puede recibir el mismo trato. Por ejemplo, si el tráfico de un vídeo y el de un correo electrónico reciben el mismo trato, los usuarios de transmisión de videos no tendrían una buena recepción de esta, mientras que los usuarios que reciben un correo electrónico no notarían tal demora, que suele ser de unos pocos segundos. Incluso los puristas de la neutralidad de la red han dejado de cuestionar este razonamiento.

Los asuntos

En el debate acerca de la neutralidad de la red, existe un emergente consenso sobre la necesidad de una gestión adecuada del tráfico. La pregunta principal es cómo determinar qué es lo adecuado. A las preocupaciones técnicas, se le suman dos áreas en las que el debate de la gestión de tráfico y la neutralidad de la red es particularmente acalorado: el aspecto económico y el de los asuntos de los derechos humanos.

El aspecto económico

Durante los últimos años, muchos operadores de red importantes – incluidos los PSI y las compañías de telecomunicaciones – han comenzado a cambiar sus modelos de negocio: además de proveer acceso a Internet a hogares y empresas, introdujeron sus propios servicios de VoIP y de IPTV, vídeo bajo demanda, portales de descarga de música o vídeo, etc. Ahora están compitiendo no solo con sus contrapartes para brindar conexiones menos costosas, más rápidas y de mejor calidad, sino también con los proveedores de servicios *over-the-top* – proveedores de servicios y contenido como Google, Facebook, Netflix, y Skype.

La gestión del tráfico puede ser una herramienta importante en la competencia de la prestación de servicios y contenido, ya que prioriza los paquetes de acuerdo con las preferencias que rigen al negocio. Por ejemplo, un operador puede decidir ralentizar o prohibir por completo que el flujo de paquetes de datos provenientes de una compañía de la competencia (como Skype o Google Voice) llegue a sus usuarios finales través de su red, mientras le da prioridad a paquetes de datos de los servicios propios (como la telefonía IP o la televisión de Internet que ofrece a sus clientes).[48]

Al mismo tiempo, los operadores afirman que la demanda de más ancho de banda – incitada mayormente por los servicios OTT – requiere de un aumento en las inversiones en la infraestructura básica. Sostienen que, debido a que los proveedores de servicios OTT son los que más contribuyen a la expansión de la demanda y los que más se benefician de la infraestructura mejorada, un modelo de política de red de varios niveles que requiera que estos proveedores contribuyan financieramente garantizaría la calidad de servicio necesaria para los clientes de los servicios OTT. Una vez más, estos casos demuestran cómo la gestión del tráfico se utiliza por razones económicas, más que técnicas.

En un intento por aumentar las ganancias, la industria de las telecomunicaciones ha diseñado nuevos modelos o acuerdos de negocio.

Los servicios a tasa cero, que los proveedores de telecomunicaciones móviles ofrecen a los clientes, permiten el uso ilimitado (gratis) de aplicaciones o servicios específicos. En algunos casos, el acceso a estas aplicaciones o servicios no se tienen en cuenta para los umbrales de datos de los suscriptores, mientras que en otros arreglos, los usuarios tienen permitido el acceso incluso sin un plan de datos. Aunque está cada vez más presente en todo el mundo, la tasación cero se ha vuelto un tema controvertido. Por un lado, algunos la consideran particularmente importante en los países en vías de desarrollo y en los menos desarrollados, en los que el acceso a los servicios de datos móviles es más costoso que el salario promedio. Uno de los argumentos principales a favor de la tasación cero es que se reducen los costos de acceso a la información en línea (cuando se ofrece dentro de un plan de datos), y brinda acceso a (parte de la) información en línea a los usuarios que no pueden costear un plan de datos (cuando el acceso es gratuito). Los defensores afirman que el acceso a parte de la información es preferible a la total falta de acceso; además, ofrecer a los

usuarios el acceso gratuito a ciertos tipos de aplicaciones podría generar la demanda del acceso a Internet en general, lo que motivaría a los operadores a invertir en la construcción y la instalación de infraestructuras.

Por otro lado, los que se oponen argumentan que la tasación cero prioriza ciertos servicios por sobre otros, y que, así, desafía al principio de neutralidad de la red y perjudica la competencia y la innovación del mercado. Algunos también expresaron su preocupación acerca de las repercusiones que la tasación cero causaría sobre los derechos humanos de los usuarios, en el sentido en que dichos servicios pueden entrar en conflicto con el derecho de acceso a la información del usuario (considerado parte del derecho más amplio de la libertad de expresión).

Los debates sobre la tasación cero se han vuelto más intensos tras la introducción del servicio *Free Basics* en 2014. Este servicio es proporcionada por Facebook en varios países en vías de desarrollo y menos desarrollados y permite a los usuarios de comunicaciones móviles acceder a aplicaciones como Wikipedia y AccuWeather (además de Facebook) sin contraer gastos de datos. Estos debates han provocado la suspensión del servicio en algunos de los países en donde se había introducido previamente (como en la India y Egipto).

A su vez, además de los servicios a tasa cero, las telecomunicaciones también hacen referencia a «servicios especializados» – como la transmisión de vídeos en HD que requieren un alto ancho de banda, o las futuras soluciones de salud electrónica – que podrían ofrecerse en un futuro y que exigirían una alta calidad y, por lo tanto, un trato especial.

Las propuestas para una Internet de varios niveles han estado en el foco de los debates sobre la neutralidad de la red por años. Una de ellas fue la Propuesta de un Marco Legislativo para una Internet abierta,[49] presentada por Verizon y Google en 2010, en la que el nivel empresarial se propuso en la forma de «servicios en línea adicionales». Los defensores de dichos modelos mantienen que esto traería más opciones de servicio para los usuarios y que motivaría la inversión en infraestructura; los opositores temen que esto vendría en detrimento de la red de mejor esfuerzo, ya que los niveles económicos y sociales realmente usarían la misma «tubería» (es decir, el cableado y el espectro inalámbrico).

Internet de múltiples niveles

El tráfico de Internet se entrega actualmente mediante el «mejor esfuerzo»: esto implica que no existen garantías en cuanto a una QoS, velocidad efectiva, o tiempo de entrega de paquetes de datos en particular. En cambio, los usuarios comparten el ancho de banda disponible y obtienen tasas de bits variables (velocidad) dependiendo de la carga del tráfico en ese momento.[50] La gestión del tráfico, por lo tanto, desempeña un papel importante en cuanto a una buena calidad de servicio para los usuarios finales.

El concepto de una Internet de múltiples niveles hace referencia a la introducción de un «nivel empresarial» en Internet; es decir, servicios especiales con una QoS garantizada además del mejor esfuerzo. Los defensores explican que el nivel empresarial funcionaría en paralelo con el económico (la Internet tal y como es ahora), que seguiría basándose en el mejor esfuerzo. Los proveedores de servicios OTT tendrían la opción de prestar sus servicios, a un costo mediante el nivel empresarial, o sin costo mediante la red del mejor esfuerzo.

Mientras tanto, el mercado produjo cambios en el funcionamiento de Internet: para reducir los costos y tiempos del tránsito, los proveedores de contenido se han acercado a los usuarios estableciendo una Red de Entrega de Contenidos (CDN, por sus siglas en inglés) – mediante el cacheo de servidores ubicados cerca de los centros regionales de Puntos de Intercambio de tráfico de Internet (IXP en inglés) o dentro de grandes empresas de telecomunicaciones regionales. Esto ha mejorado el desempeño de la red y los costos. Mientras que, en un primer momento, eran principalmente los grandes proveedores de contenidos los que podían costear (y que necesitaban) una CDN, el surgimiento de un mercado para los centros de datos y los proveedores de nube ha permitido que el servicio de CDN esté disponible en el mercado abierto. Esto habilita a cualquiera que posea un servicio a la nube y que necesite brindar el servicio a usuarios de todo el mundo a rentar los servicios de una CDN.

Asuntos de derechos humanos

Las consecuencias de violar el principio de la neutralidad de la red no son solamente económicas. La Internet se ha convertido en uno de los pilares clave de la sociedad moderna vinculada a los derechos humanos básicos, que incluyen el derecho al acceso a la información, la libertad de expresión, la salud, y la educación. Poner en peligro la apertura de Internet podría, por lo tanto, causar un impacto sobre los derechos fundamentales.

Adicionalmente, la habilidad de gestionar el tráfico de la red sobre la base de su origen o destino, servicio o contenido, podría darles a las autoridades la posibilidad de filtrar el tráfico de Internet con contenido objetable o sensible en relación con los valores políticos, ideológicos, religiosos, culturales, etc. del país. Esto da paso a la posibilidad de la censura política mediante la gestión del tráfico de Internet.

¿Usuarios o clientes?

El debate sobre la neutralidad de la red plantea también debates lingüísticos. Los defensores de la neutralidad de la red se centran en los «usuarios» de Internet, mientras que otros – más que nada los actores del sector comercial – le llaman «clientes». Los usuarios de Internet son más que meros clientes; el término «usuario» implica una participación activa en el desarrollo de Internet a través de redes sociales, blogs, y otras herramientas, y el papel fundamental que desempeñan en las decisiones sobre el futuro de Internet. Los clientes del servicio de Internet, por otro lado, como cualquier tipo de cliente, puede decidir si adquirir o no los servicios que se ofrecen. Su condición en Internet se basa en el contrato que firmaron con el PSI y en las normas de protección al cliente. Más allá de eso, se supone que los clientes no tienen ningún peso en la decisión de cómo se dirige Internet.

¿Cuáles son los principales interesados y cuáles son sus argumentos?

La posición de los principales interesados en el debate sobre la neutralidad de la red está en constante cambio. Algunos de los defensores más importantes de la neutralidad de la red incluyen a defensores de los consumidores, compañías en línea, algunas compañías tecnológicas, muchas compañías de aplicaciones de Internet como Google, Yahoo!, Vonage, eBay, Amazon, EarthLink, y compañías de *software* como Microsoft.

Los opositores a la neutralidad de la red incluyen a las principales compañías de telecomunicaciones, los PSI, los fabricantes de equipos de red y *hardware*, y los productores de contenidos

de vídeo y multimedia. Sus argumentos contra la reglamentación de la gestión del tráfico de la red se centran en el mercado, comenzando por la necesidad de ofrecer lo que quieren los clientes. A diferencia de la tendencia común de las operadoras de telecomunicaciones de oponerse a cualquier regulación sobre la neutralidad de la red, la propuesta a la CMTI-12 por parte de la Asociación Europea de Operadores de Redes de Telecomunicaciones (ETNO, por sus siglas en inglés) solicitaba una regulación internacional para evitar otras regulaciones nacionales que protegen la neutralidad de la red. Sin embargo, sus contrapartes estadounidenses – como Verizon – se oponen a la iniciativa de la ETNO.[51]

Los cuatro argumentos principales en el debate sobre la neutralidad de la red se resumen en el Cuadro 1.

Cuadro 1. Argumentos principales en el debate sobre la neutralidad de la red

Argumento	Defensores de la neutralidad de la red	Opositores a la neutralidad de la red
Argumento pasado/futuro	Nuevas compañías de Internet se establecieron gracias a la arquitectura abierta de Internet, y los usuarios finales se benefician mediante la innovación y la diversidad de servicios gracias a la neutralidad de la red. La neutralidad de la red preservará la arquitectura de Internet que ha habilitado el desarrollo rápido y novedoso de Internet hasta el momento.	La gestión del tráfico es inevitable, y la neutralidad de la red nunca existió. Además, ya existen servicios arrendados no neutrales como la VPN (Virtual private networks). Sin las restricciones de la neutralidad de la red, las compañías de Internet podrían desarrollar nuevos servicios para sus clientes, con una QoS garantizada.
Argumento económico	Sin la neutralidad de la red, la Internet será como la TV por cable: un puñado de grandes compañías controlarán el acceso y la distribución del contenido, y decidirán qué pueden ver los usuarios y cuánto les costará hacerlo. Los nuevos participantes y las pequeñas empresas no tendrán la posibilidad de desarrollarse, especialmente los de los países en vías de desarrollo. Los proveedores de servicios OTT ya pagan altos costos a las compañías de telecomunicaciones para sus conexiones de Internet, e invierten en infraestructura como los servidores de cacheo.	Sin restricciones de la neutralidad de la red en acuerdos comerciales con los proveedores de servicios y contenidos, las operadoras de telecomunicaciones serán capaces de recaudar fondos, lo que captaría su interés en invertir para desarrollar una mejor infraestructura. Una mejor infraestructura promovería nuevos servicios e innovaciones y más personalización en las necesidades de los clientes, lo que produciría más ganancias para todos. Los proveedores de servicios OTT también valorarán la posible innovación de servicios con QoS, habilitada por los operadores si no están restringidos por disposiciones sobre la neutralidad de la red.
Argumento ético	La Internet es el resultado de los desarrollos de muchos voluntarios durante décadas. Invirtieron su tiempo y creatividad en todo lo realizado, desde protocolos técnicos hasta contenido. La Internet es más que un negocio – se ha convertido en una herencia global de la humanidad. No se justifica contar con tan enorme inversión de tiempo y creatividad para que sea cosechada solamente por unas pocas compañías que cerrarán la Internet en modelos de negocios limitados violando la neutralidad de la red, y harán que la creatividad de muchos beneficie a unos pocos.	La neutralidad de la red es cuestionable desde la ética porque los operadores tienen que invertir en el mantenimiento y la expansión de la infraestructura de Internet para apoyar a los nuevos servicios, mientras que muchos beneficios van para las compañías de «contenido» de Internet, como Google, Facebook, y Amazon.
Argumento normativo	La neutralidad de la red debe estar impuesta por el gobierno para preservar el interés público. Cualquier forma de autorregulación dejará abierto el camino para que los operadores violen el principio de la neutralidad de la red. El mercado abierto no es un mecanismo suficiente dado que las principales compañías de telecomunicación globales se encuentran en el centro de la infraestructura de Internet. Incluso si existe la posibilidad de elegir, esto no siempre se lleva a cabo, ya que los usuarios necesitan la competencia y conciencia legal y técnica sobre las consecuencias de contar con muchas opciones disponibles.	La Internet se ha desarrollado gracias a la poca o directamente nula regulación. La regulación estricta por parte del gobierno podría estancar la creatividad y el futuro desarrollo de Internet. El mercado abierto está basado en la elección, y los usuarios tienen la posibilidad de que cambiar de proveedor de servicio de Internet si no están satisfechos con lo que ofrecen. La elección del usuario y el mercado acabarán con las malas ofertas y mantendrán las buenas.

Los principios básicos

En los últimos años, los debates de políticas y las regulaciones cristalizaron algunos conceptos clave para la neutralidad de la red:[52]

- Transparencia: Los operadores deben brindar información completa y precisa sobre las prácticas del manejo de sus redes, su capacidad, y la calidad de servicio que proveen a sus clientes, de una manera que sea entendible por el usuario promedio.

- Acceso: Los usuarios deben tener acceso [sin restricciones] a cualquier contenido [legal], servicio o aplicación [con una QoS mínima garantizada para el uso provechoso, según lo prescrito por el regulador] o para conectar cualquier *hardware* que no dañe a la red.

- (No)discriminación: Los operadores no deberían hacer distinciones [o solamente hacer las que sean razonables] del tráfico basándose en:

- El origen del remitente o el receptor.

- El tipo de contenido, tipo de aplicación y servicio [con una competencia justa – no discriminar a los competidores no deseados o a los servicios de los proveedores de servicios OTT.

- En los casos en los que «razonable» se refiera a cualquier práctica para el beneficio público (asegurar la QoS, la seguridad y resiliencia de la red, las innovaciones y futuras inversiones, la reducción de los costos, etc.) pero no solo para ventajas comerciales.

Otros principios que se debaten con frecuencia en los foros internacionales como el IGF global y el Diálogo Pan-Europeo sobre la Gobernanza de Internet (EuroDIG) incluyen:

- La preservación de la libertad de expresión, el acceso a la información, y la elección.

- La garantía de una QoS mínima, y la seguridad y resiliencia de la red.

- La preservación de los incentivos para las inversiones.

- La estimulación de innovaciones [incluidas las oportunidades para nuevos modelos de negocio y empresas innovadoras, es decir, nuevos participantes].

- La delimitación de los derechos, roles, y rendición de cuentas de todas las partes involucradas (proveedores, reguladores, usuarios), incluido el derecho de apelación y reparación.

- La prevención de prácticas anticompetitivas.

- La creación de un ambiente de mercado que permita a los usuarios elegir y cambiar fácilmente su operador de red.

- La protección de los intereses de los menos privilegiados, como las personas con capacidades diferentes, y los usuarios y empresas en el mundo en vías de desarrollo.

- El mantenimiento de la diversidad de contenidos y servicios.

Enfoques políticos

Con el debate de la neutralidad de la red, surgió otra pregunta: ¿Cuál es el rol de los legisladores y reguladores en las políticas de banda ancha y en las prácticas de los operadores? Uno de los mayores desafíos que enfrentan los reguladores es el de si deben actuar de manera preventiva (*ex ante*) para evitar posibles vulneraciones del principio de neutralidad de la red, o reaccionar en base a precedentes (*ex-post*) una vez que ocurra la vulneración (si es que ocurre). Otro desafío que enfrentan los legisladores y los encargados de la formulación de políticas es la dicotomía entre si deben lidiar con el problema (mediante el «derecho objetivo» – la codificación de los principios en la legislación) – o si el «derecho consuetudinario» ya resultaría suficiente (guías y políticas).[53]

Países desarrollados

En EE. UU., la Comisión Federal de Comunicaciones (FCC, por sus siglas en inglés) adoptó un conjunto de normas a favor de la neutralidad de la red. En vigencia desde junio de 2015, las normas permiten a la FCC regular los servicios de banda ancha como un servicio público y prohíben que los proveedores de banda ancha inalámbrica y por cable lleven a cabo prácticas inaceptables que la FCC considere perjudiciales para la Internet abierta: el bloqueo de contenido, aplicaciones, servicios o dispositivos legales; el impedimento o degradación de tráfico de Internet legal a causa del contenido, una aplicación o un servicio (*throttling*); y la priorización paga de ciertos contenidos, aplicaciones o servicios.[54] Los proveedores de telecomunicaciones han impugnado las normas en tribunales, argumentando que tendrían un efecto negativo en la innovación y las inversiones en la infraestructura, pero el tribunal federal de apelación denegó sus reclamos en junio de 2016.[55] Sin embargo, se espera que los proveedores continúen su «batalla» contra las reglas de la FCC.

A nivel de la UE, la regulación sobre acceso abierto a la Internet, adoptada en noviembre de 2015, establece la obligación de los proveedores de servicio de acceso a Internet de brindar el mismo trato a todo el tráfico al momento de proveer el servicio de acceso a Internet, sin discriminarlo, restringirlo, o interrumpirlo, y sin importar el emisor y el receptor, el contenido accedido o distribuido, las aplicaciones o servicios utilizados o brindados, o el equipo terminal utilizado.[56] La regulación también aborda el concepto de los «servicios especializados», y permite que los operadores ofrezcan «otros servicios además de los servicios de Internet que son optimizados por contenido, aplicaciones, o servicios específicos, o una combinación de estos, en los que la optimización es necesaria para cumplir con los requisitos del contenido, las aplicaciones o los servicios para un nivel de calidad específico». [57] En agosto de 2016, el Organismo de Reguladores Europeos de Comunicaciones Electrónicas (BEREC, por sus siglas en inglés) publicó un conjunto de lineamientos para las autoridades reguladores nacionales sobre cómo deberían implementar la regulación de la UE, incluso monitoreando de cerca y asegurando «el cumplimiento de las normas para salvaguardar el trato equitativo y no discriminativo del tráfico en la prestación de los servicios de acceso a Internet y los correspondientes derechos de los usuarios finales».[58]

Brasil, [59] Chile,[60] Eslovenia[61], y los Países Bajos[62] protegen la neutralidad de la red por medio de la legislación nacional. Noruega, por otro lado, ha decidido tomar el enfoque del derecho consuetudinario, haciendo que la autoridad reguladora nacional emita un conjunto de directrices para la neutralidad de la red (elaborado con la colaboración de varios interesados de la industria, como los PSI, organizaciones de la industria, los proveedores de contenido, y las agencias de protección del consumidor).[63]

Países en vías de desarrollo

Debido a las limitaciones del ancho de banda y la infraestructura, los reguladores de los países en vías de desarrollo se enfocan más en las políticas de uso razonable – precios accesibles y el acceso justo para todos. Algunos plantean preocupaciones sobre la no discriminación transfronteriza, y señalan que el tráfico proveniente de todos los países debería ser tratado de la misma manera, sin preferencias a raíz de los costos de terminación. Además, ciertos países poseen una mayor sensibilidad con respecto a los aspectos internos culturales, políticos, o éticos, por lo que entienden el «uso (in)adecuado» y la gestión de una manera distinta que los demás.

Se presentaron preocupaciones acerca de que los modelos innovadores de los países desarrollados podrían obstaculizar los mercados en desarrollo: al priorizar los servicios de grandes compañías de Internet, las empresas y la competencia emergentes estarían aun más minimizados, lo que amenaza la innovación, el contenido y los servicios locales, y la diversidad de los medios. Como se ha mencionado anteriormente, algunos países ya han tomado posiciones fuertes a favor de la neutralidad de la red mediante la prohibición de las prácticas de tasación cero. Otras posiciones pueden incluir el permiso para que las compañías de telecomunicaciones les cobren a los OTT globales por su prioridad, aumentando así el ingreso de las compañías de telecomunicaciones tradicionales; o, por el contrario, permitiéndoles la ejecución de la neutralidad de la red a nivel nacional para hacer que los OTT quieran operar fuera de EE. UU.

Organizaciones internacionales y ONG

Muchas organizaciones internacionales y grupos de usuarios también han definido sus posiciones políticas con respecto a la neutralidad de la red. El Consejo de Europa (CdE), en su Declaración del Comité de Ministros sobre la neutralidad de la red del 2010 y la Recomendación del Comité de Ministros sobre la protección y promoción del derecho a la libertad de expresión y el derecho a la vida privada con respecto a la neutralidad de la red del 2016 hacen hincapié en los derechos fundamentales a la libertad de expresión y a libertad de acceso a la información.[64] La Internet Society aborda la neutralidad de la red desde una perspectiva centrada en el usuario, enfocándose principalmente en los siguientes temas: permiso para la libertad de expresión, apoyo para la elección del usuario, y prevención de la discriminación.[65] El Diálogo Transatlántico de Consumidores (TACD, por sus siglas en inglés), un foro de organizaciones de EE. UU. y la UE, además hace énfasis en las solicitudes para que los prestadores asuman una conducta no discriminatoria, instando a EE. UU. y a la UE a defender los principios de apertura y la neutralidad de la red.[66] Temas como el de la neutralidad de la red y la Internet de múltiples niveles se debatieron acaloradamente dentro del proceso de la CMTI-12. El documento final de NETmundial[67] en 2014 no incluyó a la neutralidad de la red entre los principios acordados, pero invitó a un debate más profundo acerca del tema, especialmente dentro del IGF.

Muchas ONG están particularmente preocupadas por el futuro de los contenidos y servicios no comerciales y no competidores en línea, y solicitan que sean difundidos mediante cualquier prestador de red equivalente a prestadores comerciales. También hacen hincapié en los derechos de los grupos marginados – especialmente de las personas con capacidades diferentes – para usar contenido, servicios, y aplicaciones (incluso aquellos que exijan un amplio ancho de banda) para satisfacer sus necesidades sin limitaciones de ningún tipo.

Asuntos abiertos

Existe un número de asuntos abiertos en la agenda del debate sobre la neutralidad de la red:

- ¿Dónde debería estar el balance entre los efectos del bien público de Internet y los derechos de los usuarios (y los derechos humanos), por un lado, y los derechos de los proveedores de innovar dentro de las redes que les pertenece, por el otro?

- Un marco no regulado y de competencia abierta, como el que abogan los prestadores, ¿podría brindar elecciones ilimitadas (o suficientes) para los usuarios? ¿Serían capaces los usuarios de tomar decisiones significativas?[68] ¿O los reguladores deberían inevitablemente ser facultados como salvaguardas y, de ser así, con qué autoridad?

- ¿Cómo impactarían los diferentes enfoques legales y normativos sobre el mercado de banda ancha y una mayor inversión e innovación?

- ¿Cuáles son las consecuencias de la (no) neutralidad de la red para el mundo en vías de desarrollo?

- ¿Cuáles son las consecuencias de una Internet de muchos niveles para la competencia, la innovación, la inversión y los derechos humanos?

- ¿Debería considerarse que las tarifas a tasa cero o el desarrollo de CDN conforman una "Internet por niveles"?

- ¿Les parecerá a los OTT dominantes – tanto los proveedores de contenidos como los de servicios – que la Internet por niveles y los posibles nuevos servicios pueden ser también un modelo de negocio rentable? De ser así, ¿serán capaces de adaptarlo para que incluya a los usuarios de los países en vías de desarrollo, o se los dejará afuera?

- Las operadoras de telecomunicaciones, ¿pueden innovar sus modelos de negocio para incrementar sus ganancias sin violar la neutralidad de la red (siguiendo los exitosos ejemplos de iTunes, Google y otros proveedores de servicios OTT, y el potencial de asociación entre los proveedores de servicios OTT y las operadoras)?

- ¿Es posible que la necesidad de gestionar el tráfico por razones técnicas (de calidad) se vuelva obsoleta en el futuro, debido a los avances tecnológicos de los prestadores?

- ¿Cómo influirá le creciente dependencia hacia la nube y la IoT en el debate sobre la neutralidad de la red, y vice versa?

- ¿Debería extenderse el debate de la gestión del tráfico a nivel del prestador hacia la gestión de contenido y aplicaciones a nivel del prestador de contenido y aplicaciones, como Google, Apple, o Facebook?

- La protección del consumidor, ¿continuará estando intrínsecamente vinculada a la neutralidad de la red?

- Si la neutralidad de la red es «derrotada», ¿qué principios apoyarán la protección del consumidor en el futuro?

www.igbook.info/netneutrality

Estándares web y técnicos

Estándares técnicos

Los estándares técnicos de Internet aseguran que el *hardware* y el *software* desarrollado o fabricado por varias entidades no solamente puedan conectarse a Internet, sino también funcionar en conjunto tan ininterrumpidamente como sea posible. Por lo tanto, los estándares guían a la comunidad técnica, incluidos los fabricantes, hacia el desarrollo de *hardware* y *software* interoperable. Como se explicó anteriormente, el TCP/IP es el estándar técnico de Internet más importante.

El establecimiento de estándares técnicos de infraestructura

El proceso de estandarización puede llevar mucho tiempo en cualquier industria. Dado que las compañías TIC implementan nuevas tecnologías a paso acelerado, la UIT tuvo que adaptarse a las condiciones en tiempo real y, así, simplificó su volumen de trabajo de estandarización en unos pocos meses. Aun así, pueden pasar años hasta la adopción de algunos estándares importantes. Por ejemplo, la UIT espera que las redes 5G se estandaricen para el 2020.[69]

Además de la UIT, otras instituciones privadas y profesionales crean estándares técnicos cada vez con mayor frecuencia. La Junta de Arquitectura de Internet (IAB, por sus siglas en inglés) supervisa el desarrollo técnico y de ingeniería de Internet, mientras que la mayoría de los estándares son establecidos por la IETF en forma de *Requests for Comments* (RFC). Tanto la IAB como la IETF tienen su propia sede institucional dentro de la Internet Society.

Otras instituciones son el Instituto de Ingeniería Eléctrica y Electrónica (IEEE, por sus siglas en ingles), que desarrolla estándares como el Estándar WiFi (estándar IEEE 802.11b); la Wi-Fi Alliance, que es el órgano de certificación de equipos compatibles con Wi-FI; y la Groupe Speciale Mobile Association (GSMA), que desarrolla estándares para las redes móviles.

La función de establecer o implementar estándares en un mercado de tan rápido desarrollo les confiere a estas instituciones un poder de influencia considerable.

Los estándares que son abiertos (estándares abiertos de Internet) les permiten a los desarrolladores crear nuevos servicios sin la necesidad de pedir permiso. Los ejemplos incluyen a la World Wide Web y una gama de protocolos de Internet. El enfoque abierto del desarrollo de los estándares se ha visto reafirmado por varias instituciones. La iniciativa Open Stand, por ejemplo, fomenta el desarrollo de estándares abiertos y globales regidos por el mercado, y se encuentra respaldada por organismos como el IEEE, la IETF, la IAB, y la Internet Society.

Tecnología, estándares, y políticas

La importancia de establecer e implementar estándares en un mercado de rápido crecimiento les confiere a los organismos que disponen estos estándares un poder de influencia considerable.

Los estándares técnicos pueden provocar consecuencias económicas y sociales de amplio alcance, promoviendo intereses específicos y alterando el equilibrio de poder entre las

empresas en competencia y/o los intereses nacionales. Los estándares son esenciales para Internet. Por medio de ellos y del diseño de *software,* los desarrolladores de Internet pueden, por ejemplo, moldear la manera en que se usan y protegen los derechos humanos (por ejemplo, la libertad a la información, la privacidad, y la protección de datos).

Los intentos de crear estándares formales llevan a las decisiones técnicas privadas tomadas por los creadores de sistemas hacia el área pública; en este sentido, las batallas de los estándares pueden arrojar luz sobre presunciones implícitas y conflictos de interés. La pasión con la que las múltiples partes interesadas refutan las decisiones sobre los estándares nos debería advertir sobre el significado más profundo que yace debajo de los elementos básicos.

Estándares web

Los estándares web son un conjunto de estándares formales y especificaciones técnicas para la www. Aseguran que el contenido sea accesible a través de los dispositivos y las configuraciones, y, por lo tanto, proveen las reglas centrales para el desarrollo de sitios web y aplicaciones de Internet. Los principales estándares de contenido y aplicaciones incluyen HyperText Markup Language (HTML), (HTML5 es la quinta y más reciente actualización del estándar HTML), un lenguaje de texto llano que hace uso de etiquetas para definir la estructura de un documento; XML, otro tipo de lenguaje utilizado para compartir información estructurada; Cascading Style Sheets (CSS), un lenguaje utilizado en conjunción con HTLM para controlar la presentación de las páginas web; un HTML eXtensible (XHTML), una versión extendida de HTML que utiliza reglas más estrictas.

Estándares web en contexto

Para finales de la década de 1980, la batalla de los estándares de red había terminado. El TCP/IP se convirtió gradualmente en el protocolo de red principal, lo que marginó a otros estándares, como el X-25, respaldado por la UIT (parte de la arquitectura de interconexión de sistemas abiertos) y muchos estándares patentados, como la arquitectura de red de sistemas (SNA) de IBM. Si bien la Internet había facilitado la comunicación normal entre una variedad de redes mediante el TCP/IP, el sistema aún carecía de estándares de aplicaciones en común.

Tim Breners-Lee y sus colegas de la Organización Europea para la Investigación Nuclear (CERN, por sus siglas en inglés) de Ginebra brindaron una solución, que consistía en un nuevo estándar para compartir información mediante Internet, llamado HTML (que era realmente una simplificación de un estándar ISO existente, llamado SGML: el Lenguaje de Marcado Generalizado Estándar). El contenido mostrado en Internet primero debía ser organizado según los estándares HTML. El HTML, como base de la World Wide Web, abrió el camino para un crecimiento exponencial de Internet.

Desde su primera versión, el HTML ha estado en constante perfeccionamiento por medio de nuevas características. La creciente importancia de Internet hizo que la cuestión sobre la estandarización del HTML se ubicara como un tema central. Esto fue especialmente relevante durante la Guerra de los Navegadores entre Netscape y Microsoft, en la que cada compañía intentó reforzar su posición en el mercado mediante la influencia sobre los estándares HTML. Aunque los HTLM básicos solo manipulaban textos y fotografías, las nuevas aplicaciones de Internet exigían tecnologías más sofisticadas para la gestión de bases de datos, vídeos y animaciones. Dicha variedad de aplicaciones exigió esfuerzos de

estandarización considerables para asegurar que el contenido de Internet pudiera ser visto por la mayoría de los navegadores de Internet.

La estandarización de las aplicaciones entró en una nueva fase con el surgimiento de XML, que brindó mayor flexibilidad en el establecimiento de estándares para el contenido de Internet. También se introdujeron nuevos conjuntos de estándares XML. Por ejemplo, el estándar para la distribución de contenido inalámbrico se llama Lenguaje de Marcado Inalámbrico (WML, por sus siglas en inglés).

Establecimiento de estándares web

La institución que encabeza el establecimiento de estándares es W3C, dirigida por Tim Berners-Lee. Los estándares se desarrollan mediante un elaborado proceso que tiene como finalidad promover el consenso, la imparcialidad, la rendición de cuentas pública, y la calidad. Tras la amplia construcción del consenso, se publican los estándares mediante «Recomendaciones».[70]

Los estándares del W3C definen una plataforma abierta para el desarrollo de aplicaciones, que habilita a los desarrolladores a construir ricas experiencias interactivas. El W3C indica que «si bien los límites de la plataforma continúan evolucionando, los líderes de la industria se pronuncian casi al unísono sobre cómo HTML5 será el pilar fundamental para esta plataforma».[71]

Cabe mencionar que a pesar de su gran relevancia para la Internet, hasta ahora, el W3C no ha atraído mucha atención en el debate sobre la gobernanza de Internet.

www.igbook.info/standards

Informática en la nube

Qué es y cómo funciona la informática en la nube

La informática en la nube (*cloud computing*) puede describirse como la transición del almacenamiento de datos en discos rígidos en nuestras computadoras hacia el almacenamiento de datos en los servidores en la nube (es decir, enormes torres de servidores). La informática en la nube facilita el acceso ubicuo a nuestros datos y servicios desde cualquier dispositivo en cualquier parte del mundo (siempre y cuando haya conexión a Internet). A su vez, el hecho de que nuestros datos se encuentren almacenados con un tercero – a menudo en pedazos y copias esparcidas a lo largo de varias jurisdicciones – plantea preocupaciones en cuanto a la privacidad y la protección de datos. La nube tiene la posibilidad de ser mucho más segura que nuestras computadoras, ya que las brechas de seguridad a nivel de los sistemas en la nube podrían proporcionar acceso a grandes cantidades de datos (Figura 9).

La primera ola de la informática en la nube comenzó con el uso de los servidores de correo en línea (Gmail, Yahoo!), las aplicaciones de redes sociales (Facebook, Twitter) y aplicaciones en línea (Wikis, blogs, Google Docs). Además de las aplicaciones diarias, la informática en la nube es usada de manera extensiva en los *softwares* de negocios. Nuestras posesiones digitales están trasladándose cada vez más desde nuestros discos rígidos hacia la nube. Los

Figura 9. Informática en la nube

principales actores en la informática de la nube son Google, Microsoft, Apple, Amazon, y Facebook, quienes ya tienen grandes torres de servidores o planean desarrollarlas.

De alguna manera, la informática en la nube cerró el círculo del desarrollo de la tecnología informática. Durante los primeros días de las computadoras, existían computadoras centrales poderosas y terminales «bobas». El poder se ubicaba al centro, en los servidores poderosos. La transición del poder desde los servidores poderosos hacia las terminales de los usuarios finales se llevó a cabo cuando las compañías como IBM, Apple, y Microsoft comenzaron a fabricar computadoras personales. El poder de las computadoras se trasladó a las computadoras en todas partes del mundo. Así, empezamos a almacenar los datos en disquetes y discos rígidos, y a ejecutar aplicaciones (desde procesadores de textos hasta juegos) en nuestras computadoras. Luego, las tecnologías de la red comenzaron a conectar estas computadoras individuales, primero dentro de las compañías y organizaciones (mediante Redes de Área Local [LAN]) y después de manera global, mediante, particularmente, la Internet. En la etapa temprana del crecimiento público de Internet (hasta el 2005), la Internet se utilizaba más que nada para el intercambio de datos, mientras que los datos se almacenaban en nuestras computadoras, que también ejecutaban aplicaciones de *software* incorporadas, como los procesadores de texto. Otra transición comenzó con el crecimiento de las redes sociales y el surgimiento de los teléfonos inteligentes y las tabletas durante los últimos 10 años. Al mismo tiempo, el *software* y los datos empezaron a trasladarse desde nuestras computadoras hacia poderosos servidores en la nube. Este proceso tuvo su comienzo con los servicios de correo electrónico como Gmail, y continuó con el almacenamiento de fotos, archivos de texto, y otros recursos digitales en la nube, y operando el *software* de la nube con mayor frecuencia también (como Google Docs o Microsoft Office 365). Actualmente, la mayoría de nuestras posesiones digitales son almacenadas en

servidores centralizados en la nube. En cierto modo, cerramos el círculo que comenzó con una arquitectura de red centralizada temprana, pasando por las computadoras personales descentralizadas, y terminamos con el almacenamiento centralizado en la nube.

Una configuración de la nube consiste de tres capas: *hardware, middleware* o plataforma, y *software* de aplicación. Según lo que rente el usuario, existen tres tipos de servicios en la nube:

- El software como servicio (SaaS, por sus siglas en inglés), en el que un proveedor de servicios en la nube brinda a los usuarios acceso a las aplicaciones de *software*, permitiendo así que el usuario acceda a tales aplicaciones (así como también a los datos que estas produjeron) desde cualquier dispositivo conectado a Internet. El usuario no tiene control sobre ninguno de los recursos de la nube, sino que solamente puede hacer uso de la aplicación disponible. Este es el tipo de servicio más dominante en el que la aplicación del usuario final es un punto de entrada para su uso – como en el caso de Twitter o una aplicación para la base de datos central en una organización local.

- La plataforma como servicio (PaaS, por sus siglas en inglés), en la que los usuarios mismos pueden desarrollar una aplicación que opere en la plataforma de la nube rentada. De esta forma, el usuario puede decidir sobre los recursos de *hardware* que quieran usar en particular; sin embargo, siguen sin tener la posibilidad de ajustar la configuración del servidor o del almacenamiento. La estandarización es importante especialmente con respecto a la plataforma, debido a que habilita a los desarrolladores a dirigirse a una amplia gama de consumidores potenciales, y les da a los usuarios la posibilidad de elegir.

- La infraestructura como servicio (IaaS, por sus siglas en inglés) es el servicio en la nube menos utilizado entre la población en general, ya que exige ciertas habilidades sobre TI avanzadas para su uso, aunque da lugar a la mayor libertad de elección con respecto a la manera en que se pueden usar los recursos. En la IaaS, el proveedor solamente brinda recursos de *hardware* (poder computacional o de almacenamiento), mientras que el usuario es quien debe establecer los servicios, incluido el sistema operativo.

Aspectos políticos y legales sobre la informática en la nube

Los servidores de la nube como una infraestructura de información crítica

La mayoría de las aplicaciones de Internet operan a partir de servidores de la nube. En la era previa a la nube, cuando Internet se caía, el daño se limitaba a la falta de la disponibilidad del servicio – no podíamos enviar correos electrónicos o navegar en la web. En la era de la informática en la nube, puede que no seamos capaces de escribir textos o hacer cálculos, dado que estas tareas se llevan a cabo mediante aplicaciones basadas en la nube. La gran relevancia de los servicios de la nube para millones de usuarios de Internet y compañías hace que los servidores de la nube formen parte de la infraestructura crítica a nivel global y en la mayoría de las sociedades alrededor del mundo.

Seguridad y cifrado

El simple hecho de que un solo operador de la nube provea un servicio para miles o millones de personas es suficiente para atraer la atención de muchos delincuentes – criminales, terroristas, ciberespías, u otros – para explotar vulnerabilidades.

Las posibles vulneraciones de la seguridad de la nube se pueden clasificar según la reconocida tríada de la seguridad de la información: confidencialidad, integridad, y disponibilidad (CIA en inglés) de los datos y del sistema. A tal efecto, hacer que la nube sea segura significa la consideración de un conjunto de medidas como: decidir sobre los derechos de acceso a segmentos de datos y servicios específicos, cifrar el conjunto de datos en la nube en su totalidad, asegurar cada segmento del sistema TIC y la red entre la nube y los usuarios, cifrar la transferencia de datos entre la nube y los usuarios finales, y hacer un respaldo de todos los datos almacenados en la nube (Figura 10).

La privacidad y la protección de datos

Al almacenar cada vez más nuestros datos personales en las nubes, los interrogantes sobre la privacidad y la protección de datos se vuelven cruciales. ¿Tendremos el control de nuestros archivos de texto, correos electrónicos, y otros datos? ¿Podría suceder que los operadores de la nube utilicen nuestros datos sin nuestro consentimiento? ¿Quién tendrá acceso a nuestros datos?

La UE está particularmente involucrada en los asuntos sobre la privacidad y la protección de datos en el contexto de la informática en la nube. Debido a que más y más datos cruzan el Océano Atlántico, la UE y EE. UU. han intentado hacer frente al problema de los distintos regímenes de privacidad, asegurando a su vez que los operadores de la informática en la nube de EE. UU. cumplan con las regulaciones de protección de datos y privacidad de los ciudadanos de la UE. Se supone que el remplazo del acuerdo de Safe Harbour (declarado con carácter nulo por el TJUE en octubre de 2015) por el Escudo de Privacidad (formalmente adoptado en julio de 2016) debería solucionar el problema, pero aún queda por ver cuán efectivo será el nuevo acuerdo.

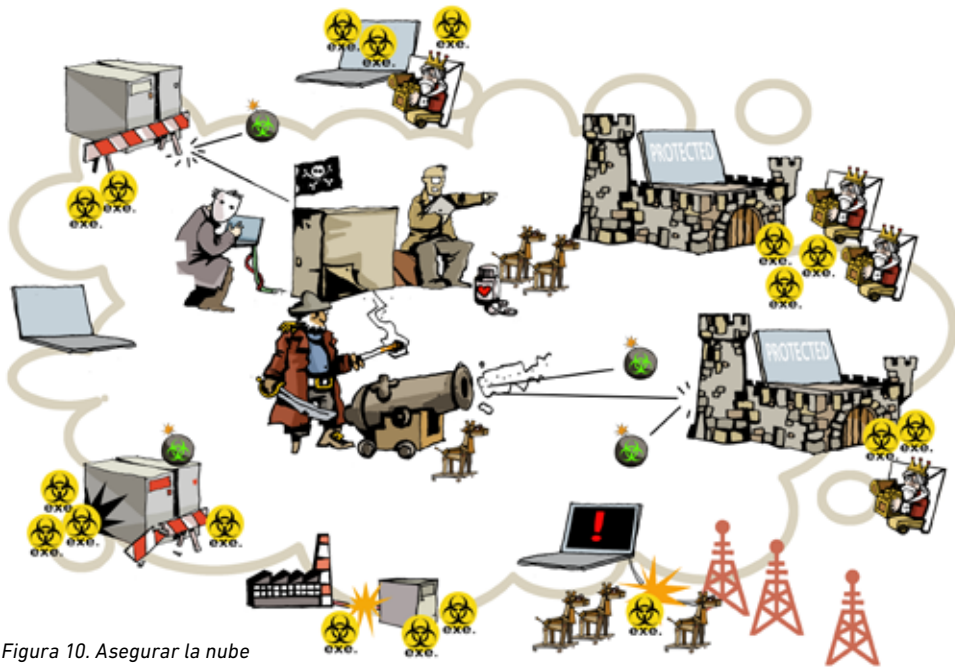

Figura 10. Asegurar la nube

Big data

La mayor parte del fenómeno big data está relacionada con la informática en la nube. Aunque exista un gran revuelo sobre el big data, este fenómeno es enormemente importante en los desarrollos digitales modernos. Particularmente, el big data obtendrá una nueva relevancia con el rápido crecimiento de la Internet de las cosas, en la que los automóviles, los electrodomésticos, e incluso la ropa comenzará a recopilar datos. El big data propulsará un nuevo tipo de modelo económico. También propulsará una nueva demanda de recursos de la nube.

Por ejemplo, se está desarrollando la computación en la niebla (*fog computing*) como un adicional a la computación en la nube, con el objetivo de reducir la cantidad de datos que se transfieren a la nube para su procesamiento y análisis. Como lo explica Cisco, la computación en la nube acerca más la nube a las «cosas» que producen y accionan sobre los datos; esto permite que los datos sean analizados más cerca de donde se recopilaron o produjeron, minimizando así la latencia[72], descargando gigabites de tráfico de la red a partir de la red central, y conservando los datos sensibles dentro de la red.[73]

Localización de datos

Debido al creciente volumen de información convertida a formato digital, los países se están incomodando con el hecho de tener los activos de datos nacionales fuera de los límites regionales. Algunos de ellos están adoptando, o explorando la posibilidad de adoptar, políticas que imponen normas para la localización de datos (que exigen que los proveedores de servicios en la nube y/o los datos que almacenan estén localizados dentro de las fronteras nacionales).

Las motivaciones para la localización de datos varían, desde razones económicas hasta políticas. La localización de datos motivada por razones económicas está basada a menudo en una política económica proteccionista. Si se considera que los datos son el recurso clave de la economía de Internet, los países tratarán de conservar este recurso dentro de sus territorios y fomentar el desarrollo de una economía local en base al procesamiento y la gestión de datos. La protección de datos y las consideraciones sobre seguridad también pueden hacer que los gobiernos exijan que ciertos datos sean procesados y almacenados dentro de sus países, lo que haría que la legislación nacional sea directamente aplicable a los proveedores de servicios. Además, los países también han comenzado a explorar la idea de instalar nubes gubernamentales, diseñadas específicamente para el procesamiento y almacenamiento de datos oficiales/gubernamentales. Las razones políticas para las normas de localización de datos están vinculadas a los intereses de algunos países de controlar el activismo político, lo que, se podría decir, es más fácil de conseguir cuando el país tiene jurisdicción sobre los servidores de datos en línea.

Los proveedores de servicios de la nube están intentando encontrar soluciones, incluso técnicas, para paliar las políticas de localización, mientras que ofrecen a sus clientes la posibilidad de aprovechar los servicios de la nube. A modo de ejemplo, en marzo de 2016, Oracle lanzó un nuevo servicio de informática en la nube que permitiría que las empresas coloquen servidores de nube de Oracle dentro de sus propios centros de datos. Según Oracle, el nuevo servicio está destinado a satisfacer las necesidades que tienen las organizaciones que hasta ahora no han adoptado la informática en la nube debido a los requisitos legislativos y normativos relacionados con la localización de los servidores de la nube.[74]

Estándares e interoperabilidad

La cuestión de los estándares se volvió muy importante a causa de los diversos operadores de informática en la nube. Los estándares son sumamente importantes para la

interoperabilidad y la transferencia de datos entre distintas nubes (por ejemplo, de Google a Apple). Una posibilidad que se está debatiendo es la de la adopción de estándares abiertos por parte de los principales actores en la informática de la nube. No obstante, esto no es fácil de lograr, ya que las compañías de informática en la nube más importantes consideran que sus estándares patentados son parte de su ventaja en la competencia. Sin embargo, existen varias iniciativas destinadas a lograr la interoperabilidad. Por ejemplo, en 2013, el Open Group (con miembros como Fujitsu, IMB, y Oracle) publicó una Guía para la portabilidad e interoperabilidad de la informática en la nube, que contenía recomendaciones para los usuarios sobre cómo lograr la portabilidad e interoperabilidad al trabajar con productos y servicios de la nube, así como también consejos para los proveedores y órganos de estandarización sobre cómo los estándares y las mejores prácticas deberían evolucionar para dar paso a una mejor portabilidad e interoperabilidad.[75] El IEEE creó la iniciativa de Informática en la Nube IEEE, que se dedica, entre otras cosas, a desarrollar estándares para la operabilidad entre nubes.

www.igbook.info/cloud

La Internet de las cosas

La IoT extiende la conexión a Internet principalmente desde los dispositivos de comunicación e información (computadoras, teléfonos móviles, tabletas, y libros electrónicos) hacia otros dispositivos como los automóviles, los electrodomésticos, la ropa, la infraestructura urbana, y los dispositivos médicos y del cuidado de la salud.

Se estima que la cantidad de dispositivos conectados a la IoT para el 2020 varíe entre 20 y 100 mil millones. Estos dispositivos generarán grandes cantidades de datos particularmente valiosos para el análisis. La Corporación Internacional de Datos (IDC, por sus siglas en inglés) previó que, para el año 2020, el «universo digital» llegará a 44 ZB (zettabytes, es decir, un billón de gigabites), y el 10% de la cantidad total provendría de los dispositivos de la IoT.[76]

Crecen las predicciones sobre el desarrollo financiero de la industria de la IoT y los planes de los fabricantes están aumentando exponencialmente. Verizon prevé que el mercado mundial de la IoT crecerá significativamente durante los próximos años, desde $591.7 mil millones en 2014 hasta $1.3 billones en 2019, con una tasa de crecimiento anual compuesto del 17%.[77]

Un informe que publicaron la UIT y Cisco Systems a principios de 2016 concluye que la IoT es una oportunidad de desarrollo importante que puede mejorar los estándares de vida en todo el mundo y contribuir sustantivamente con el logro de los objetivos de desarrollo sustentable. El informe describe el creciente impacto que tiene la IoT en áreas como el cuidado de la salud, la educación, el agua y saneamiento, la resiliencia, el cambio climático y la mitigación de la contaminación, el empleo de los recursos naturales y la energía.[78]

Los dispositivos de la IoT están a menudo conectados en sistemas amplios, a las que se las denomina «casas inteligentes» o «ciudades inteligentes». Tales dispositivos generan enormes cantidades de datos y también crean nuevos contextos en los que estos datos pueden ser utilizados. Los dispositivos de la IoT utilizan la actual estructura de Internet, no una Internet separada/distinta.

Los sensores y piezas más comunes utilizados para la comunicación de los dispositivos de la IoT son los siguientes:

- Identificadores de radiofrecuencia (RFID en inglés): etiquetas electrónicas conectadas a productos para habilitar el seguimiento. Puede utilizarse para el transporte/seguimiento de ropa, mascotas, cajas.

- Códigos Universales de Producto (UPC, por sus siglas en inglés): se utilizan en casi todos los productos en el escaneo que se lleva a cabo en las cajas en los supermercados.

- Códigos Electrónicos de Productos (EPC, por sus siglas en inglés): brindan una identidad única para cada objeto físico de cualquier parte del mundo en todo momento. Los EPC funcionan como los UPC, con la excepción de los primeros son electrónicos.

Además de estos, los investigadores continúan explorando otros métodos de conexión para los dispositivos de la IoT. Por ejemplo, en un documento publicado en junio de 2016,[79] un grupo de investigadores propone el uso de lámparas LED (diodos emisores de luz) para la conexión de los dispositivos en la IoT. Afirman que este sistema podría ser la solución a los desafíos de comunicación en el espectro radioeléctrico saturado (dado que muchos dispositivos IoT ahora dependen del uso de radiofrecuencias).

Aun si el tamaño de un solo pedazo de datos generado por dispositivos conectados a la IoT podría ser bastante pequeño, la suma final es impactante debido al número de dispositivos que se pueden conectar, y al hecho de que los datos se pueden almacenar y procesar en la nube. Por lo tanto, la industria de la informática en la nube desempeñará un rol importante en los futuros desarrollos de la IoT.

Industrias de la IoT

Algunas de las industrias más desarrolladas de la IoT son:

- La automatización doméstica: provee acceso a los electrodomésticos desde cualquier parte. No existe un protocolo unificado, ni ningún estándar web API para la industria.

- Monitoreo de la salud: facilita la nivelación de la salud de manera activa (bombas de insulina controladas de manera remota por médicos, monitoreo de marcapasos, etc.). También crea datos sobre los ciclos o hábitos de una persona, aunque existen posibles problemas de seguridad y la carga de datos arbitraria.

- Transporte: brinda la posibilidad del uso de los sistemas de la IoT para llevar un registro de información sobre el uso de combustible, la ubicación, el tiempo, y la distancia, y para anticipar las necesidades de mantenimiento en vehículos, y optimizar el uso de recursos (incluso flotas). Yendo un poco más lejos, los automóviles sin conductor, que es tema de investigación de los fabricantes de automóviles (como Tesla y Toyota), así como también compañías como Google y Uber, también hacen uso de las tecnologías de la IoT.

Otras industrias en las que la IoT está teniendo un peso cada vez mayor son: la industria de la energía, de la infraestructura, de la agricultura, de la fabricación, y de las aplicaciones para los consumidores. El concepto en general de las «ciudades inteligentes» (en las que las TIC están integradas en los servicios e infraestructuras urbanos para mejorar su calidad y desempeño y aumentar los estándares generales de la vida urbana) está estrechamente relacionado también con la ioT.

Iniciativas privadas y públicas

El sector comercial está llevando a cabo las mayores iniciativas en cuanto a la IoT. Mientras que compañías tecnológicas como Cisco e Intel continúan desarrollando sus carteras de servicios de la IoT, los proveedores de servicios de telecomunicaciones ya han comenzado a emplear redes dedicadas a la IoT a gran escala, para fomentar el uso de la IoT.[80] Además, compañías de distintos sectores están uniendo sus fuerzas y formando alianzas destinadas a contribuir más con los desarrollos en el campo de la IoT. Un ejemplo es la fundación Open Connectivity Foundation, cuyo objetivo es contribuir con la garantía de que los dispositivos de la IoT se puedan comunicar entre sí, sin importar cuál sea su fabricante, sistema operativo, chipset, o transporte físico. Esta fundación abarca a miembros de distintos sectores, como el automovilístico, la electrónica de consumo, el cuidado de la salud, el industrial, etc. Otro ejemplo es la alianza LoRa Alliance, que opera en el campo de la estandarización de la IoT. La alianza desarrolló LoRaWAN: una especificación de redes amplias de bajo consumo (LPWAN, por sus siglas en inglés) destinada a brindar una interoperabilidad continua entre los objetos de la IoT.

Los gobiernos también están tomando conciencia sobre las oportunidades que la IoT trae aparejadas, por lo que varios tipos de iniciativas están siendo lanzadas en esta área. La UE, por ejemplo, inició el Programa de Trabajo de Horizonte 2020 para 2016/2017: Los Pilotos a Gran Escala para la Evaluación e Implementación de la Internet de las Cosas, un programa de financiación dedicado a la promoción de la adopción de la IoT en Europa. En EE. UU., la NTIA ha estado investigando el panorama tecnológico y político de la IoT, en el afán de identificar posibles roles para el gobierno federal en la promoción del avance tecnológico de la IoT en asociación con el sector privado. El gobierno de China creó el Instituto de Tecnología de la Internet de las Cosas Chengdu, mediante el cual financia la investigación de varias áreas relacionadas con la IoT.

Los asuntos principales

El IoT genera enormes cantidades de datos, lo que ha provocado importantes preocupaciones relacionadas con la privacidad y la protección de datos. Algunos dispositivos de la IoT pueden recopilar y transmitir datos que son de carácter personal (por ejemplo, el caso de los dispositivos médicos de la IoT), y existen inquietudes sobre la protección de los aparatos en sí (la garantía de que sean seguros)[81], así como también sobre cuántos de los datos que recopilan son procesados y analizados. Mientras que la información transmitida mediante un dispositivo de la ioT puede no causar problemas con la privacidad, cuando los conjuntos de datos recopilados desde múltiples dispositivos se juntan, procesan y analizan, esto puede llevar a la revelación de información sensible.

La ausencia de la supervisión de datos también plantea el problema de la propiedad de los datos. Muchas de las aplicaciones utilizadas en la IoT están patentadas, junto con los datos creados y generados mediante ellas. Puede que se necesiten nuevas regulaciones, debido a que existen reparaciones en la seguridad y la privacidad (de datos, protocolos, y dispositivos). Este es un futuro desarrollo que quizás exija una regulación y acción global unificada, posiblemente más que cualquier otro ámbito de la gobernanza de Internet. Se necesita celebrar nuevos contratos sociales.

Surgieron cuestiones éticas debido a que la IoT está en el centro de las iniciativas de inteligencia artificial que buscan introducir robots, automóviles sin conductor, y otros sistemas digitales que deben emitir juicios y tomar decisiones. Los gobiernos y el sector privado

están instando cada vez más al diálogo sobre los principios éticos que deberían aplicar a los desarrollos en el campo de la IoT y la IA, y sobre cómo podrían incorporarse estos principios en los sistemas de la IoT y la IA.

Asuntos éticos

La IoT, el big data y la IA hacen que aparezca la ética en el centro de las políticas digitales. Las inquietudes éticas no están solamente relacionadas con la privacidad y la seguridad, sino también con la ética de las decisiones tomadas por máquinas automatizadas. Por ejemplo, Jigsway, una subsidiaria de Google, desarrolló *Conversation AI,* un conjunto de herramientas destinadas a encontrar abusos y acosos en Internet. Aunque potencialmente hace frente a problemas relacionados con el uso indebido del espacio público de Internet, este *software* también plantea un problema ético importante: ¿Cómo pueden determinar las máquinas cuál es un lenguaje apropiado y cuál no? [82]

El debate sobre las implicaciones éticas de las nuevas tecnologías digitales comenzó tanto en el sector comercial como en el de políticas. Grandes compañías de Internet (IBM, Facebook, Google, Microsoft, Amazon, y DeepMind) lanzaron una iniciativa denominada Partnership on Artificial Intelligence, dedicada al abordaje de la privacidad, seguridad y desafíos éticos de la IA, y a la introducción de un diálogo social más amplio sobre los aspectos éticos de los nuevos desarrollos digitales.[83] Un proyecto de informe sobre la robótica, preparado en el Parlamento Europeo durante el primer semestre de 2016 explora, entre otras cosas, los desafíos éticos impuestos por los desarrollos tecnológicos en el área de la robótica, y recomienda la adopción de un «un marco ético que sirva de orientación en materia de diseño, producción y uso de robots», «basándose en principios de beneficencia , no maleficencia y autonomía, así como en los principios [...] como la dignidad humana y los derechos humanos, la igualdad, la justicia y la equidad, la no discriminación y la no estigmatización [...]».[84] En EE. UU., el Plan Nacional Estratégico para el Desarrollo y la Investigación de la Inteligencia Artificial, lanzado en octubre de 2016, enfatiza la necesidad de «determinar la manera de diseñar una mejor estructura para los sistemas de IA que incorporan el razonamiento ético».[85] Un informe sobre robótica y la IA elaborado por el Comité de Ciencia y Tecnología en el Parlamento del Reino Unido insta al gobierno a tomar medidas proactivas para enfrentar las cuestiones éticas relacionadas con el uso de tecnologías autónomas como la IA.[86]

www.igbook.info/iot

Convergencia

Históricamente, la telecomunicación, la radiodifusión, y otras áreas relacionadas, eran industrias separadas; utilizaban diferentes tecnologías y estaban regidas por diferentes reglamentaciones. El uso amplio y predominante de Internet ayudó en la convergencia de las plataformas tecnológicas para la telecomunicación, radiodifusión, y la entrega de información. Actualmente, podemos hacer llamadas telefónicas, mirar TV, y compartir música desde nuestras computadoras mediante la Internet. Hace unos pocos años, dichos servicios estaban bajo el manejo de distintos sistemas tecnológicos.

En el campo de las telecomunicaciones tradicionales, el principal punto de convergencia es el VoIP. La creciente popularidad de los sistemas de VoIP como Skype, WhatsApp, y Viber está basada en un precio reducido, la posibilidad de integrar líneas de datos y comunicación por voz, y el uso de herramientas avanzadas, basadas en dispositivos móviles o computadoras personales. Gracias a YouTube y servicios similares, la Internet está también en convergencia con los servicios multimedia y de entretenimiento tradicionales. El IPTV también converge entre los servicios multimedia y las redes basadas en IP.

Aunque la convergencia técnica lleva la delantera a un ritmo acelerado, sus consecuencias económicas y legales requerirán tiempo para evolucionar.

A nivel internacional, los mecanismos de gobernanza son usados principalmente por el intercambio de mejores prácticas y experiencias en el campo de la convergencia. El Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D) cuenta con un grupo de estudio sobre el ambiente de convergencia. El CdE cuenta con un comité directivo sobre los medios y la información, que cubre un aspecto de la convergencia: la interacción entre los medios tradicionales y los nuevos medios digitales. La convergencia está asociada directamente con la neutralidad de la red, la IoT, el papel de los intermediarios, el comercio electrónico, la protección del consumidor, y los impuestos.

Los asuntos

Las implicaciones económicas de la convergencia

A nivel económico, la convergencia ha comenzado a darle una nueva forma a los mercados tradicionales colocando a compañías que previamente operaban en dominios separados en competencia directa. Como consecuencia, la convergencia ha resultado en temores del «síndrome Uber» entre los líderes empresariales: un panorama en el que un competidor con un modelo de negocio completamente distinto entra a la industria y arrasa con la competencia.[87] Ese fue el caso de Uber cuando se introdujo en el mercado de los taxis innovando en el aspecto tecnológico; consecuentemente, las compañías de taxis tradicionales y los conductores, que sintieron una amenaza para sus negocios, presentaron demandas en los tribunales por todo el mundo en protesta contra el nuevo participante del mercado, que no estaba regulado.

Las compañías utilizan distintas estrategias para enfrentar los desafíos que impone la convergencia. Un enfoque frecuente ha sido la fusión y la adquisición: cuando se trata de compañías pequeñas, otras compañías más grandes adquieren o se fusionan con proveedores de servicios OTT que son nuevos en el mercado. En un enfoque más reciente, los proveedores de servicios OTT y los de telecomunicaciones han comenzado a establecer asociaciones, que traen ventajas para ambas partes: para los proveedores de telecomunicaciones, las sociedades con los proveedores de servicios OTT puede brindarles una ventaja competitiva, así como también un valor agregado para los usuarios finales; los proveedores de servicios OTT, por otro lado, tendrían a sus servicios en una posición más fácil de encontrar y acceder, gracias a la sociedad con las prestadoras.[88]

La regulación en el ambiente de convergencia

El sistema legal es el más lento para amoldarse a los cambios causados por la convergencia tecnológica y económica. Cada segmento – telecomunicación, radiodifusión, y entrega de información – tiene su propio marco normativo especial. Esta convergencia causó varias preguntas sobre la gobernanza y la reglamentación:

- ¿Qué pasará con los regímenes nacionales e internacionales existentes en los campos como la telefonía y la radiodifusión?

- ¿Se necesita un nuevo régimen normativo que se concentre principalmente en los servicios que convergen? O, ¿deberían estar sujetos a los mismos marcos normativos que, por ejemplo, los servicios tradicionales de comunicación electrónica?

- Cuando se trata de la competencia y la protección del consumidor, ¿qué reglas, si las hubiere, deberían imponerse para los proveedores de los servicios que convergen?

- ¿Deberían ser las autoridades públicas (estados y organizaciones internacionales) las que lleven a cabo la regulación de dicha convergencia, o debería ser autorregulada?

Los países están abordando estas preguntas de varias maneras. Algunos, como los miembros de la UE, la India, y Kenia, escogieron enfoques flexibles con respecto a la regulación de la convergencia, simplemente abordando los problemas en función de los principios de la neutralidad de la red, ya que los usuarios tienen la posibilidad de elegir cualquier tipo de aplicación o servicio ofrecido mediante las redes IP. Otros países eligieron crear nuevos marcos normativos o jurídicos para los servicios en convergencia: Corea, por ejemplo, cuenta con una ley denominada «Internet Multimedia Broadcasting Business Act», que contiene disposiciones sobre los requisitos de licenciamiento y las obligaciones de servicio para el IPTV. En algunos otros países, la convergencia se aborda mediante la autorregulación. En Australia, por ejemplo, la alianza Communications Alliance (que representa a varias compañías en la industria de las comunicaciones) elaboró varios lineamientos para los servicios VoIP.[89]

Existen, sin embargo, varios países en los que los servicios en convergencia, especialmente los de VoIP, están (o estuvieron, en algún momento) explícitamente prohibidos mediante regulaciones, o simplemente bloqueados por los proveedores de servicios de telecomunicaciones. Algunos ejemplos son Marruecos, Belice, y los Emiratos Árabes Unidos, entre otros.

www.igbook.info/convergence

NOTAS FINALES

[1] Los términos «Internet» y «www» a veces se usan indistintamente; sin embargo, hay una diferencia. La Internet es una red de redes conectada por TCP/IP. A veces, el término «Internet» abarca la infraestructura, la aplicación (correo electrónico, ftp, web), y el contenido. El «www» es una de las tantas aplicaciones de Internet, un sistema de documentos intervinculados, conectados con la ayuda del Protocolo de Transferencia de Hipertexto (HTTP, por sus siglas en inglés).

[2] De conformidad con una política de neutralidad tecnológica, la UE ha estado utilizando el término «comunicaciones electrónicas» en lugar de «telecomunicaciones». Esto cubre, por ejemplo, el tráfico de Internet sobre la red eléctrica, que no forma parte de la infraestructura de telecomunicaciones.

[3] Las Comunicaciones mediante Línea de Potencia (PLC, por sus siglas en inglés) permiten la transmisión de datos de Internet a través de la red eléctrica. Dada su profunda capilaridad, el uso de la red eléctrica haría de la Internet un medio más accesible para muchos usuarios. Para una revisión técnica y organizacional de este mecanismo, por favor diríjase a: Palet J (2003) *Addressing the Digital Divide with IPv6-enabled Broadband Power Line Communication,* Internet Society, Informe de miembro No. 13 de la ISOC. Disponible en http://www.isoc.org/briefings/013 [accedido el 7 de octubre de 2016].

[4] El proyecto Loon de Google tiene como finalidad incrementar la cobertura de banda ancha y llegar hasta las áreas más remotas del mundo que no tienen ninguna infraestructura de telecomunicación. La compañía lanzará numerosos globos a la estratósfera, a aproximadamente 20 kilómetros por sobre la superficie, y cada uno actuará como una estación base flotante proveedora de señal para los usuarios finales. Estos globos están conectados entre sí y a las estaciones base en la superficie mediante enlaces de alta velocidad, brindados por las operadoras de telecomunicaciones asociadas.

[5] Según la UIT, los Espacios en Blanco de Televisión (TVWS, por sus siglas en inglés) son «porciones no utilizadas del espectro de TV, a las que también se conoce como espectro entrelazado». Dado que las frecuencias no utilizadas pertenecen a una parte del espectro que habilita la «ventajosa propagación de las propiedades inherentes del espectro UHF [TV] (excelente cobertura exterior e interior y propiedades de propagación sin línea de vista)», como explica Cristian Gómez del Buró de Radiocomunicación de la UIT, los TVWS son considerados como la tecnología alternativa de amplia gama y de bajo consumo que puede funcionar tanto para las aplicaciones de banda ancha en zonas rurales como para la comunicación entre máquina y máquina (M2M), importantes para la aplicación de la IoT. Para más información, por favor consulte: UIT (2012) Dividendo Digital: Insights for Spectrum Decisions. Disponible en http://www.itu.int/ITU-D/tech/digital_broadcasting/Reports/DigitalDividend.pdf [accedido el 7 de octubre de 2016], y Gomez C (2013) Espacios en Blanco de Televisión: Managing spaces or better managing inefficiencies? Disponible en http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR_paper_WhiteSpaces_Gomez.pdf [accedido el 18 de julio de 2016].

[6] La liberalización de los mercados de telecomunicación de los miembros de la OMC se formalizó en 1998 en el Convenio de Telecomunicaciones Básicas (BTA, por sus siglas en inglés). Tras la adopción del BTA, más de 100 países iniciaron el proceso de liberalización, caracterizado por la privatización de monopolios de telecomunicaciones nacionales, la introducción de competencia, y el establecimiento de autoridades reguladoras nacionales. El Convenio lleva el nombre formal de *Cuarto protocolo anexo al Acuerdo General sobre el Comercio de Servicios* (adoptado el 30 de abril de 1996 y vigente desde el 5 de febrero de 1998. Disponible en http://www.wto.org/english/tratop_e/serv_e/4prote_e.htm [accedido el 7 de octubre de 2016].

[7] UIT (sin fecha) Signatarios de las Actas Finales – CMTI-12. Disponible en http://www.itu.int/osg/wcit-12/highlights/signatories.html [accedido el 7 de octubre de 2016].

[8] Para obtener más información sobre las actividades de la UIT en relación con Internet, visite http://www.itu.int/osg/csd/intgov/ [accedido el 7 de octubre de 2016].

[9] La Arquitectura de Identificación de Objetos Digitales – un proyecto iniciado por Robert Kahn (uno de los inventores del TCP/IP) – tiene como objetivo asociar identificadores únicos a cada objeto digital (datos y servicios). Se pretende que dichos identificadores no sufran cambios, sin perjuicio del lugar en el que se ubique dentro de las redes, de quién sea su dueño, o en qué tecnología tengan su base, etc. Mientras que la responsabilidad del manejo de aspectos relacionados con la DOA recae sobre la Fundación DONA, con base en Suiza, la UIT, mediante los grupos de estudio del Sector de Telecomunicaciones, ha estado explorando la posibilidad de adoptar la DOA como estándar para la computación en la nube y los dispositivos de la IoT. Mientras que algunos Estados miembros de la UIT abogan por la adopción de los estándares de la DOA, y brindan razones como la de la lucha contra la falsificación de dispositivos, existen opiniones que afirman que, al permitir el rastreo de los dispositivos, podría abusarse de la DOA para también rastrear y controlar el flujo de información, así como también las acciones de los usuarios. Para obtener más detalles, diríjase a: Corporación para Iniciativas Nacionales de Investigación (2010) A Brief Overview of the Digital Object Architecture and its Application to Identification, Discovery, Resolution and Access to Information in Digital Form. Disponible en http://www.cnri.reston.va.us/papers/Digital_Object_Architecture_Brief_Overview.pdf [accedido el 20 de octubre de 2016]; Javed D (2016) ITU IoT Standards: Gateway to Government Control? Disponible en http://www.wileyconnect.com/home/2016/9/20/itu-iot-standards-gateway-to-government-control [accedido el 20 de octubre de 2016]

[10] Para obtener más información sobre el rol de la OMC en el campo de las telecomunicaciones, visite http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm [accedido el 7 de octubre de 2016].

[11] Esta sección está basada en: Kurbalija J (2016) From Harmonising Cyberpolicies to Promoting Twiplomacy: How Diplomacy Can Strengthen Asia-Europe's Digital Connectivity. Fundación Asia-Europa (ASEF, por sus siglas en inglés). *Informe Prospectivo 2016/2017 de la ASEF. Connectivity: Facts and Perspectives, Volume II: Connecting Asia and Europe*. Disponible en http://www.asef.org/images/docs/ASEF%20Outlook%20Report%202016-2017%20Vol2.pdf [accedido el 20 de octubre de 2016].

[12] UNESCAP (2014) Discussion Paper Series on Problems and Challenges in Transit Connectivity Routes and International Gateways in Asia. *Serie de Documentos de Discusión,* 2014/1. Disponible en http://www.unescap.org/sites/default/files/Discussion%20Paper-Transit-Connectivity_0.pdf [accedido el 20 de octubre de 2016].

[13] Verda M (2014) Superautopista Transeuroasiática de la Información. Disponible en http://sam.az/uploads/PDF/TRANS-EURASIAN%20INFORMATION%20SUPER%20HIGHWAY.pdf [accedido el 20 de octubre de 2016].

[14] El término «Ruta de Seda Digital» se usa informalmente como un concepto general que abarca varios proyectos de cooperación entre Asia y Europa en el campo digital. Para obtener más información, diríjase a: Jia L and Shuang G (2015) Digital Silk Road to span Eurasia, *China Daily Europe*, 10 de julio. Disponible en http://europe.chinadaily.com.cn/epaper/2015-07/10/content_21241323.htm [accedido el 20 de octubre de 2016]; y Zhao Huanxin Z (2015) Web companies asked to support 'digital Silk Road,' *China Daily Europe*, 8 de septiembre. Disponible en http://www.chinadaily.com.cn/business/2015chinaarabforum/2015-09/08/content_21823475.htm [accedido el 20 de octubre de 2016]. La Ruta de Seda Digital es parte de la iniciativa Un Cinturón, Una Ruta (yidai-yilu), que consiste en el Cinturón Económico de la Ruta de la Seda terrestre que debería cruzar el continente y la Ruta de Seda Marítima que conecte a China con las regiones marítimas del Sudeste Asiático, el sur de Asia, Medio Oriente, África del Este, y el Mediterráneo. Se planea que el proyecto total cruce 60 países de una población total de 4,4 mil millones, que representa el 63% de la población mundial. Para obtener más detalles, consulte: Arase D (2015) China's Two Silk Roads Initiative: What It Means for Southeast Asia. *Southeast Asian Affairs* 41, pp. 25-45; y Tsao R (2015) Un cinturón una ruta: Una perspectiva histórica. *Chinese American Forum* 31(1) pp. 11-14.

[15] Para obtener más información sobre la política del espectro electromagnético de la UE, visite http://ec.europa.eu/digital-agenda/en/what-radio-spectrum-policy [accedido el 7 de octubre de 2016].

[16] En las redes informáticas, el *peering* es la interconexión voluntaria de redes de Internet separadas de manera administrativa con el propósito de intercambiar el tráfico entre los consumidores

de cada red. La definición más fiel del término es libre de acuerdos o «el emisor se queda con todo», lo que significa que ninguna de las partes paga a la otra el tráfico intercambiado; en lugar de eso, cada uno obtiene ganancias a partir de sus propios clientes. El *peering* exige la interconexión física de las redes y un intercambio de información del encaminamiento mediante el protocolo *Border Gateway* (de enrutamiento de puerta de enlace de borde – BGP, por sus siglas en inglés). Usualmente, viene acompañado por acuerdos de intercambio de tráfico de diversa formalidad, desde acuerdos informales hasta contratos elaborados. (Fuente: Wikipedia).

17 Los IBP del Nivel 2 se denominan generalmente Puntos de Conexión de Internet (ICP, por sus siglas en inglés) o portales de Internet.

18 Spaink K (2002), en *Freedom of the Internet, our new challenge,* menciona dos casos relacionados. Disponible en http://www.spaink.net/english/osce_internetfreedom.html [accedido el 7 de octubre de 2016]. En el primer caso, la acción legal estuvo dirigida contra una página web con contenido Nazi cuestionable, alojada por Flashback en Suecia. Los tribunales decidieron que la página no violaba las leyes suecas antinazis. No obstante, un activista antinazi comprometido con la causa montó una fuerte campaña contra Flashback, lo que puso en aprietos al PSI de Flashback, Air2Net, y al principal operador de red troncal MCI/WorldCom. Bajo la presión de dicha campaña, MCI/WorldCom decidió desconectar a Flashback a pesar de la falta de fundamentos legales para hacerlo. Los intentos de Flashback por conseguir un proveedor alternativo no tuvieron éxito, ya que muchos de ellos estaban también conectados mediante la red troncal operada por MCI/WorldCom. El segundo caso tuvo lugar en los Países Bajos. Un pequeño PSI holandés, Xtended Internet, fue desconectado por su *upstream provider* (el proveedor que está más arriba en la escala) estadounidense bajo la presión generada por la Cienciología.

19 Metz C (2016) Facebook y Microsoft tenderán un cable gigante que atravesará el Atlántico. *Wired Magazine*, 26 de mayo. Disponible en http://www.wired.com/2016/05/facebook-microsoft-laying-giant-cable-across-atlantic/ [accedido el 7 de octubre de 2016].

20 La IANA se describe a sí misma como una de las instituciones de Internet más antiguas. Sus funciones datan de la década de 1970, las cuales eran desempeñadas por una sola persona: Jon Postel, quien en ese momento era científico informático en la Universidad de California del Sur. Desde comienzos de 1998, las funciones de IANA han sido desempeñadas por ICANN, sobre la base de un contrato con el gobierno de EE. UU. Tras el vencimiento de dicho contrato, el 1 de octubre de 2016, las funciones continuaron bajo la responsabilidad de ICANN, por medio de una subsidiaria – PTI – creada recientemente. Las funciones de IANA se pueden agrupar en tres categorías: nombres de dominios (administración de la raíz DNS, los dominios .int y .arpa, y un recurso de prácticas de nombres de dominio internacionalizados [IDN]), recursos de números (la coordinación del repositorio global de números IP y Autónomos, fundamentalmente brindándolos a los RIR), y la asignación de protocolos (la administración de los sistemas numéricos del protocolo de Internet se lleva a cabo en tándem con organismos de estandarización). Para obtener más información, visite https://www.iana.org/about [accedido el 7 de octubre de 2016].

21 Los RIR actuales son: ARIN (el Registro Estadounidense para Números de Internet), APNIC (Centro de Información de Redes de Asia y el Pacífico), LACNIC (el Registro de Direcciones de Internet para América Latina y el Caribe), RIPE NCC (el Centro de Coordinación de Redes IP Europeas – que cubre Europa y el Medio Oriente) y AFRINIC (Centro de Información de Redes para África). Para obtener una explicación detallada del sistema RIR, visite https://www.ripe.net/participate/internet-governance/internet-technical-community/the-rir-system [accedido el 7 de octubre de 2016].

22 Drake W *et al.,* La fragmentación de Internet: Una visión general. Disponible en http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf [accedido el 7 de octubre de 2016].

23 Por ejemplo, en el 2000, la IETF elaboró la RFC 2893, Mecanismos de Transición para *hosts* y enrutadores IPv6, que describe los mecanismos de transición que «permitirán que los nodos del IPv6 mantengan una completa compatibilidad con el IPv4, lo que debería simplificar enormemente el empleo del IPv6 en la Internet, y facilitar la eventual y completa transición de Internet hacia el IPv6». Disponible en https://www.ietf.org/rfc/rfc2893.txt [accedido el 7 de octubre de 2016].

24 Tras un evento exitoso del Día Mundial de IPv6 que tuvo lugar el 8 de junio de 2011, los PSI más importantes, los fabricantes de equipos de redes domésticas, y las compañías web de todas

partes del mundo se reunieron para habilitar de manera permanente el IPv6 para sus productos y servicios para el 6 de junio de 2012: el Lanzamiento Mundial de IPv6. En 2016, cuatro años después de su lanzamiento, se informó que el tráfico global del IPv6 había crecido más de un 500%. Para obtener más detalles, visite http://www.worldipv6launch.org [accedido el 7 de octubre de 2016].

[25] Para un estudio más completo y altamente técnico de la seguridad del protocolo TCP/IP, diríjase a: Chambers C *et al.,* (sin fecha) TCP/IP Security, Departamento de Ciencia de la Computación y de la Información. Universidad Estatal de Ohio. Disponible en http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html [accedido el 7 de octubre de 2016].

[26] Bavisi J (2011) What Security Issues does IPv6 Pose? *eSecurity Planet.* Disponible en http://www.esecurityplanet.com/trends/article.php/3935356/What-Security-Issues-Does-IPv6-Pose.htm [accedido el 25 de julio de 2016].

[27] Ashford W (2011) IPv6: The security risks to business. *Computer Weekly,* 29 de agosto. Disponible en http://www.computerweekly.com/feature/IPv6-The-security-risks-to-business [accedido el 26 de julio de 2016].

[28] Para obtener más detalles sobre el grupo, visite http://www.etsi.org/technologies-clusters/technologies/next-generation-protocols [accedido el 7 de octubre de 2016].

[29] Uno de los pocos documentos de referencia sobre el DNS es la RFC 1591 (de marzo de 1994), que especifica la estructura de gobernanza del DNS. Disponible en https://www.ietf.org/rfc/rfc1591.txt [accedido el 7 de octubre de 2016].

[30] ICANN (2016) Estatutos para la Corporación para la Asignación de Nombres y Números de Internet. Disponible en https://www.icann.org/resources/pages/governance/bylaws-en [accedido el 7 de octubre de 2016].

[31] Para ver una lista con los Acuerdos de Registros actuales, visite https://www.icann.org/resources/pages/registries/registries-agreements-en [accedido el 7 de octubre de 2016].

[32] Los registradores que quieren brindar servicios de registración de nombres de dominio bajo gTLD, con acceso directo a los registros de los gTLD, necesitan que ICANN los acredite. Para ver una lista de estos registros visite https://www.icann.org/registrar-reports/accredited-list.html [accedido el 7 de octubre de 2016].

[33] Para ver estadísticas sobre los nuevos gTLD, y una lista de las cadenas delegadas, visite https://newgtlds.icann.org/en/program-status/statistics [accedido el 7 de octubre de 2016].

[34] El informe de la IANA sobre el dominio de nivel superior con código de país para Palestina está disponible en http://www.iana.org/reports/2000/ps-report-22mar00.html [accedido el 7 de octubre de 2016].

[35] Para conocer más detalles sobre los registros para los ccTLD, vea la Base de Datos de la Zona Raíz de IANA, disponible en http://www.iana.org/domains/root/db [accedido el 7 de octubre de 2016].

[36] El modelo brasilero de la gestión de los dominios de país generalmente se presenta como un ejemplo exitoso de un enfoque de múltiples partes interesadas. El órgano nacional a cargo de los dominios brasileros está abierto a todos los actores clave, incluso a las autoridades gubernamentales, el sector comercial, y la sociedad civil. Para obtener más información, por favor consulte: Alfonso C (2004) BR: CCTLD, Un bien de interés público, en MacLean D (ed) *Internet Governance: A Grand Collaboration*. Nueva York: Fuerza de Trabajo TIC de la ONU, pp. 291–299; los fragmentos están disponibles en http://books.google.ro/books?id=pEFAypES4t0C&printsec=frontcover&hl=ro#v=onepage&q&f=false [accedido el 14 de octubre de 2016].

[37] Por ejemplo, Sudáfrica usó sus derechos de soberanía como argumento para retomar el control de su dominio de país. Se adoptó una ley que especifica que el uso del dominio de país fuera de los parámetros prescriptos por el gobierno sudafricano sería considerado un delito. La transición de Camboya del dominio de país desde el control del sector no gubernamental hacia el gobierno se cita a menudo como ejemplo de una transición no exitosa. El gobierno redujo la calidad de los servicios e impusó tarifas más elevadas, lo que hizo que la registración de los dominios de Camboya fuera mucho más difícil. Para obtener más información, lea a Klien N (2004) Internet Governance: Perspectives from Cambodia en MacLean D (ed) *Internet Governance: A Grand Collaboration.* Nueva York: Fuerza de Trabajo TIC de la ONU, pp. 227-237. Los fragmentos están disponibles en http://books.google.ro/books?id=pEFAypES4t0C&printsec=frontcover&hl=ro#v=onepage&q&f=false [accedido el 7 de octubre de 2016].

[38] Para conocer más detalles sobre la delegación y redelegación de un ccTLD, diríjase a la guía sobre la Delegación o redelegación de un dominio de nivel superior con código de país (ccTLD) de la IANA. Disponible en http://www.iana.org/help/cctld-delegation [accedido el 7 de octubre de 2016].

[39] GAC de ICANN (2005) Principios para la Delegación y Administración de los Dominios de Nivel Superior con Código de País. Disponible en https://gacweb.icann.org/display/GACADV/ccTLDs?preview=/28278844/28475457/ccTLD_Principles_0.pdf [accedido el 14 de octubre de 2016].

[40] El archivo de la zona raíz está disponible al público en http://www.iana.org/domains/root/files [accedido el 7 de octubre de 2016].

[41] Para ver la lista de los servidores de la zona raíz, sus nodos y posiciones, y las organizaciones que los gestionan, visite http://www.root-servers.org/ [accedido el 7 de octubre de 2016].

[42] Para ver la lista de las 13 autoridades nombradas en la zona raíz del DNS, visite http://www.iana.org/domains/root/servers [accedido el 9 de octubre de 2016].

[43] ISC Inc. (2003) Hierarchical Anycast for Global Distribution. Disponible en http://ftp.isc.org/isc/pubs/tn/isc-tn-2003-1.html [accedido el 14 de octubre de 2016].

[44] Para obtener más detalles, diríjase a Das D (2015) Lista de los 4 mejores servidores DNS alternativos a tu ISP. Disponible en http://www.snaphow.com/4402/list-of-top-4-alternative-dns-servers-to-your-isp/ [accedido el 7 de octubre de 2016].

[45] Para obtener más detalles sobre el Yeti DNS Project, visite https://yeti-dns.org [accedido el 7 de octubre de 2016].

[46] Para un análisis completo de los desafíos relacionados con los sistemas raíz alternativos, diríjase a Bertola V (sin fecha) Oversight and multiple root server systems. Disponible en http://wgig.org/docs/book/Vittorio_Bertola.html [accedido el 7 de octubre de 2016].

[47] Las tecnologías de transmisión de señal – tanto la inalámbrica, como la *Long Term Evolution* (LTE), y los cables ópticos, como *Dense Wavelength Division Multiplexing* (DWDM) – prometen resolver el problema del «agotamiento del ancho de banda» con especificaciones de ancho de banda mucho más grandes (hasta terabits por segundo). Sin embargo, el problema entre la oferta y la demanda será perpetuo.

[48] *The Economist* (2009) America insists on net neutrality: The rights of bits. 24 de septiembre. Disponible en http://www.economist.com/node/14517422 [accedido el 7 de octubre de 2016].

[49] Para ver el texto completo de la Propuesta de Verizon y Google para un Marco Legislativo para una Internet Abierta, visite http://www.google.com/googleblogs/pdfs/verizon_google_legislative_framework_proposal_081010.pdf [accedido el 7 de octubre de 2016].

[50] El ancho de banda (tasa de bits) que se acordó mediante contrato con el PSI es, de hecho, solamente el máximo disponible en lugar de una velocidad efectiva garantizada.

[51] McCullagh D (2012) European ISPs defend U.N. Internet tax. *C|net*, 20 de agosto. Disponible en http://news.cnet.com/8301-13578_3-57496581-38/european-isps-defend-u.n-Internet-tax/ [accedido el 7 de octubre de 2016].

[52] Los elementos que todavía son controvertidos y que se negociarán en el futuro se encuentran entre corchetes.

[53] Radunović V (2012) Net Neutrality in law – a step forwards or a step backwards? Diplo Blog. Disponible en http://www.diplomacy.edu/blog/network-neutrality-law-%E2%80%93-step-forwards-or-step-backwards [accedido el 14 de octubre de 2016].

[54] Comisión Federal de Comunicaciones (2015) Orden de Internet Abierta. Disponible en https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf [accedido el 8 de agosto de 2016].

[55] El caso cayó en manos del Tribunal de Apelación de EE. UU. para el Circuito del Distrito de Columbia, y el fallo del Tribunal está disponible en https://www.cadc.uscourts.gov/Internet/opinions.nsf/3F95E49183E6F8AF85257FD200505A3A/$file/15-1063-1619173.pdf [accedido el 14 de octubre de 2016].

[56] Parlamento Europeo, Consejo de la Unión Europea (2015) Regulación (UE) 2015/2120 del Parlamento Europeo y del Consejo del 25 de Noviembre de 2015 que establece las medidas relativas al acceso a una Internet abierta y que modifica la Directiva 2002/22/EC sobre el servicio

universal y los derechos de los usuarios que se relacionan con las redes y servicios de comunicaciones electrónicas y la Regulación (UE) No. 531/2012 sobre el servicio itinerante de las redes públicas de comunicaciones móviles dentro de la Unión. Disponible en http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015R2120 [accedido el 8 de agosto de 2016].

[57] En junio de 2016, cuando el BEREC publicó un borrador de los conjuntos de lineamientos sobre cómo los entes reguladores nacional debían implementar las nuevas normas de neutralidad de la red, grandes proveedores de telecomunicaciones europeos reaccionaron argumentando que los lineamientos propuestos «crearían incertidumbres significativas sobre el retorno de la inversión del 5G». Explicaron que el 5G introduce el concepto de «capas lógicas de la red» (*network slicing*), que tiene el propósito de permitir una gran variedad de modelos de negocio de la industria en una plataforma en común, y con garantías de servicio. Desde ese punto de vista, la propuesta es «excesivamente prescriptiva y podría hacer que las empresas de telecomunicaciones se rehúsen a asumir riesgos, obstaculizando así la explotación del 5G, ignorando la agilidad fundamental y la naturaleza elástica de las capas lógicas de la red 5G para adaptarse en tiempo real a los cambios en la demanda de los usuarios finales/aplicaciones y el tráfico». Otras entidades, como la Unión Europea de Radiodifusión, están en desacuerdo con esta opinión, y consideran que las normas sólidas de la neutralidad de la red serán la clave para el desarrollo de una «plataforma de tecnología 5G abierta e interoperable». Para obtener más detalles, diríjase a Patterson G *et al.* (2016) Manifiesto para la implementación oportuna del 5G en Europa. Disponible en http://telecoms.com/wp-content/blogs.dir/1/files/2016/07/5GManifestofortimelydeploymentof5GinEurope.pdf [accedido el 9 de agosto de 2016]; y la respuesta de la Unión Europea de Radiodifusión a la consulta pública del borrador del BEREC sobre los lineamientos para la implementación de las normas de la neutralidad de la red. Disponible en http://www.ebu.ch/files/live/sites/ebu/files/Publications/Position%20Papers/EBU_response_BEREC_consultation_NN_guidelines_final_version_18072016.pdf [accedido el 9 de agosto de 2016].

[58] Organismo de Reguladores Europeos de Comunicaciones Electrónicas (2016) Directrices para la implementación de las reglas de neutralidad de la red por parte de las autoridades nacionales europeas. Disponible en http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules [accedido el 7 de octubre de 2016].

[59] La versión en inglés del Marco Civil está disponible en http://www.giplatform.org/resources/text-brazilsnew-marco-civil [accedido el 8 de octubre de 2016].

[60] TechnoLlama (2012) Chile enforces net neutrality for the first time, sort of. Disponible en http://www.technollama.co.uk/chile-enforces-net-neutrality-for-the-first-time-sort-of [accedido el 8 de octubre de 2016].

[61] European Digital Rights (2013) Slovenia has a net neutrality law. Disponible en https://edri.org/edrigramnumber11-2slovenia-net-neutrality/ [accedido el 8 de agosto de 2016].

[62] Electronic Frontier Foundation (2012) The Netherlands passes net neutrality legislation. Disponible en https://www.eff.org/deeplinks/2012/05/netherlands-passes-net-neutrality-legislation [accedido el 8 de agosto de 2016].

[63] Autoridad Noruega de Comunicaciones (2009) Guidelines for Internet neutrality. Disponible en http://eng.nkom.no/technical/Internet/net-neutrality/net-neutrality/_attachment/9222?_ts=1409aa375c1 [accedido el 7 de octubre de 2016].

[64] El texto completo de la Declaración del Comité de Ministros sobre la neutralidad de la red de 2010 está disponible en https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805ce58f [accedido el 9 de agosto de 2016]. El texto de la Recomendación del Comité de Ministros sobre la protección y promoción del derecho a la libertad de expresión y el derecho a la vida privada con respecto a la neutralidad de la red está disponible en https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/ec(2016)1&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383&direct=true [accedido el 9 de agosto de 2016].

[65] Internet Society (sin fecha) Neutralidad de la Red. Disponible en http://www.internetsociety.org/net-neutrality [accedido el 3 de noviembre de 2016].

[66] TACD (2015) Resolution on the open and neutral Internet. Disponible en http://tacd.org/wp-content/uploads/2015/06/TACD-INFOSOC-Resolution-on-Net-Neutrality-2015-GREEN.pdf [accedido el 3 de noviembre de 2016].

[67] Reunión Global de Múltiples Partes Interesadas sobre el Futuro de la Gobernanza de Internet (2014) Declaración de Múltiples Partes Interesadas de NETmundial. Disponible en http://netmundial.br/netmundial-multistakeholder-statement/ [accedido el 14 de octubre de 2016].

[68] Radunović V (2012) Can free choice hurt open Internet markets? Diplo Blog. Disponible en https://www.diplomacy.edu/blog/can-free-choice-hurt-open-Internet-markets [accedido el 7 de octubre de 2016].

[69] Unión Internacional de Telecomunicaciones (2016) La UIT hacia «IMT para 2020 y más allá». Disponible en http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx [accedido el 7 de octubre de 2016].

[70] La lista actualizada de estándares de Internet actuales, estándares de borrados, y estándares propuestos en el directorio de Estándares Oficiales de Protocolos de Internet está disponible en https://www.rfc-editor.org/standards [accedido el 7 de octubre de 2016].

[71] El Consorcio de la World Wide Web (sin fecha) Estándares. Disponible en http://www.w3.org/standards/ [accedido el 14 de octubre de 2016]

[72] La latencia hace referencia a la cantidad de tiempo que demora que un paquete de datos llegue, desde un punto designado, hasta otro punto dentro de la red.

[73] Cisco (2015) Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. Disponible en https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf [accedido el 7 de octubre de 2016].

[74] Oracle (2016) Oracle presenta una nueva cartera de servicios para ayudar en la simplificación de la adopción de la nube por parte de compañías globales. Disponible en https://www.oracle.com/corporate/pressrelease/oracle-cloud-at-customer-032416.html [accedido el 7 de octubre de 2016].

[75] The Open Group (2013) Portabilidad e Interoperabilidad de la Informática en la Nube. Disponible en http://www.opengroup.org/cloud/cloud_iop/ [accedido el 7 October 2016].

[76] IDC (2014). El universo digital de las oportunidades: Información valiosa y el aumento del valor de la Internet de las cosas. Disponible en http://www.emc.com/leadership/digital-universe/2014iview/digital-universe-of-opportunities-vernon-turner.htm [accedido el 7 de octubre de 2016]

[77] Verizon (2016) State of the Market: Internet of Things 2016. Disponible en http://www.verizon.com/about/our-company/state-of-the-market-Internet-of-things [accedido el 7 de octubre de 2016].

[78] ITU and Cisco Systems (2016) Harnessing the Internet of Things for Global Development. Disponible en http://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf [accedido el 7 de octubre de 2016].

[79] Schmid S *et al.* (2016) EnLighting: An Indoor Visible Light Communication System Based on Networked Lights Bulbs. Disponible en https://s3-us-west-1.amazonaws.com/disneyresearch/wp-content/uploads/20160615205959/EnLighting-An-Indoor-Visible-Light-Communication-System-based-on-Networked-Light-Bulbs-Paper.pdf [accedido el 7 de octubre de 2016].

[80] En los Países Bajos, se empleó una red nacional dedicada a las soluciones de la IoT (LoRa) en julio de 2016 por parte de una compañía de telecomunicaciones holandesa. En Corea del Sur, Samsung y SK Telecom han estado trabajando en el lanzamiento de una red comercial dedicada a la IoT a lo largo del país.

[81] En septiembre-octubre de 2016, dos grandes ataques DDoS, que utilizaron muchos dispositivos IoT, hizo que algunos de los principales sitios web fueran inaccesibles. Más de un millón de dispositivos fueron utilizados en ataques contra un investigador de seguridad estadounidense y un proveedor de servicios de red francés. El segundo ataque fue dirigido a sistemas operados por el proveedor de servicios DNS Dyn, que sufrió tres ataques en un día; los ataques afectaron a Twitter, PayPal, Netflix, Airbnb, Amazon, CNN, y varias revistas en línea. Para obtener más información, consulte Rash W (2016) Weak device security surns IoT into powerful weapon in DDos attacks. *Eweek*, 1 de octubre de 2016. Disponible en http://www.eweek.com/security/weak-device-security-turns-iot-into-powerful-weapon-in-ddos-attacks.html [accedido el 12 de noviembre de 2016]. *Wikipedia* (2016) 2016 Dyn ciberataque. Disponible en https://en.wikipedia.org/wiki/2016_Dyn_cyberattack [accedido el 12 de noviembre de 2016].

[82] Greenberg A (2016) Inside Google's Internet Justice League and its AI-powered war on trolls. *Wired*, 19 de septiembre. Disponible en https://www.wired.com/2016/09/inside-googles-Internet-justice-league-ai-powered-war-trolls/ [accedido el 20 de octubre de 2016].

[83] Romm T (2016) Tech companies launch new AI coalition. *Politico, 11 de octubre. Disponible en* http://www.politico.com/story/2016/10/tech-companies-launch-new-ai-coalition-229600 [accedido el 20 de octubre de 2016].

[84] Comisión de Asuntos Jurídicos del Parlamento Europeo (2016) Proyecto de informe con recomendaciones para la Comisión sobre normas de Derecho Civil sobre Robótica. Disponible en http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2015/2103(INL)&l=en [accedido el 7 de octubre de 2016].

[85] Consejo estadounidense Nacional sobre Ciencia y Tecnología (2016) Plan Nacional Estratégico para el Desarrollo y la Investigación de la Inteligencia Artificial. Disponible en https://www.whitehouse.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf [accedido el 20 de octubre de 2016].

[86] Comisión del Parlamento del Reino Unido sobre Ciencia y Tecnología (2016) Robótica e Inteligencia Artificial. Disponible en http://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14502.htm [accedido el 20 de octubre de 2016].

[87] IBM Institute for Business Value (2016) Redefining Boundaries. Insights from the Global C-suite Study. Disponible en https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03695usen/GBE03695USEN.PDF [accedido el 7 de octubre de 2016].

[88] Para obtener más detalles sobre las asociaciones entre los proveedores de telecomunicaciones y los proveedores OTT, refiérase a: Body of European Regulator for Electronic Communications (2016) Report on OTT services. Disponible en http://www.stibbe.com/~/media/03%20news/newsletters/brussels/bru%20tmt%20berec%20report%20on%20ott%20services.pdf [accedido el 7 de octubre de 2016].

[89] Para obtener más detalles sobre los variados enfoques jurídicos y normativos con respecto a la convergencia, lea: UIT, infoDev (sin fecha) El impacto de la convergencia. Disponible en http://www.ictregulationtoolkit.org/6.4 [accedido el 7 de octubre de 2016].

Sección 3

LA CANASTA DE SEGURIDAD

La canasta de seguridad

Ciberseguridad

La Internet se diseñó originalmente para el uso de un círculo cerrado de, más que nada, académicos. La comunicación era abierta. La seguridad no era una preocupación.

La ciberseguridad apareció en el centro de la escena debido a la expansión de Internet más allá del círculo de pioneros. La Internet repitió la vieja paradoja de que la tecnología puede ser tan habilitante como amenazante. Lo que puede usarse para el provecho de la sociedad también puede usarse para su perjuicio.

La Internet moderna, con más de 3 mil millones de usuarios, es la infraestructura crítica (CI) de la sociedad actual. La vulnerabilidad de Internet es la vulnerabilidad de la sociedad moderna. El sector financiero, los servicios gubernamentales, el sector de la seguridad, las escuelas, y los hospitales dependen cada vez más de la interconectividad y de la red global, de una manera irreversible; esto también les sucede a los ciudadanos.

Además, las tensiones políticas entre los países se reflejan en el ciberespacio, y a veces causan ciberincidentes. Los ciberincidentes – especialmente los relativos a la CI – pueden acarrear consecuencias funestas para la funcionalidad del estado, la economía, y el bienestar; por ejemplo, un ciberataque a escala nacional en Suiza podría representar la pérdida de más de €500 millones por día.[1]

Mapeo de ciberseguridad

Los asuntos de ciberseguridad se pueden clasificar de acuerdo con tres criterios:

- Tipo de acción. La clasificación basada en el tipo de acto puede incluir la intercepción de datos, la interferencia de datos, el acceso ilícito, el *software* espía, la corrupción de datos, el sabotaje, la denegación de servicio (DoS), y la usurpación de la identidad.

- Tipo de delincuente. Los posibles delincuentes pueden ser criminales, anarquistas, hacktivistas, revolucionarios, terroristas, servicios secretos, y unidades militares y de defensa.

- Tipo de objetivo Los posibles blancos son numerosos: desde individuos, compañías privadas, organizaciones de la sociedad civil, entidades mediáticas, e instituciones públicas, hasta la infraestructura central de Internet (operadoras de telecomunicaciones, PSI, IXP y centros de datos), la infraestructura crítica de la sociedad (suministros de energía y agua, instalaciones industriales, tráfico, etc.), y recursos militares.

El marco de ciberseguridad incluye principios de políticas, instrumentos, e instituciones que abordan el tema. La ciberseguridad es un término general que cubre varias áreas:

- La protección de la infraestructura crítica de la información (CIIP, por sus siglas en inglés) es cada vez más importante porque la CI, incluidos la energía, el agua, las

comunicaciones, y las finanzas, ahora dependen de Internet y de otras redes informáticas que funcionan como la infraestructura de información subyacente. La infraestructura de información crítica (CII, por sus siglas en inglés) incluye no solo los equipos y enlaces (cuya seguridad se denomina de manera general como seguridad de la red), sino que también los protocolos, centros de datos, y los recursos críticos de Internet.

- La ciberdelincuencia es el crimen cometido mediante la Internet y sistemas informáticos. Incluye: los antiguos, es decir, crímenes tradicionales que ahora se cometen por medio del ciberespacio (como muchos fraudes), crímenes que evolucionaron a causa de la tecnología (por ejemplo, el fraude con tarjetas de crédito, y el abuso y explotación sexual de niños en línea), nuevos crímenes que emergieron con Internet (por ejemplo, ataques DoS y el fraude de pago por clic), y la comercialización de herramientas de ciberdelincuencia – distribuidas más que nada mediante mercados negros en línea – que se utilizan para facilitar otros crímenes (por ejemplo, los virus y *botnets*). La lucha contra el abuso y la explotación sexual infantil en Internet es el área más desarrollada de la cooperación internacional contra la ciberdelincuencia. Aumentar la seguridad de todos los usuarios, y particularmente de los niños – lo que se conoce como seguridad en Internet – más que nada mediante la educación y la concientización, es un importante campo de prevención de crímenes, estafas, o acoso.

- Los ciberconflictos, comúnmente conocidos como la ciberguerra, son altamente visibles en los medios, pero cuentan con un bajo nivel de atención política y jurídica. La cooperación en relación con los ciberconflictos se divide en tres grandes áreas: desarrollo de los ciberconflictos (es decir, ¿pueden aplicarse las leyes existentes, principalmente Las Convenciones de La Haya, al ciberespacio?; de no ser así, ¿qué tipo de instrumento legal nuevo debería desarrollarse?); armas y desarmamiento (es decir, cómo introducir ciberarmas en el proceso de desarmamiento); y el derecho humanitario (es decir, cómo aplicar los Convenios de Ginebra a los ciberconflictos). El ciberespionaje económico, los hackeos que habilitan el filtrado de documentos políticos, y las actividades de sabotaje que entran dentro de la categoría de actos de guerra están quedando primeros en la agenda política y diplomática. El aumento del uso de Internet por parte de terroristas para la información, comunicación, propaganda y atentados – a veces denominado «ciberterrorismo» – a menudo se enmarca de manera política, como un problema de seguridad nacional y mundial, aunque su persecución recae sobre la legislación penal nacional.

Amenazas a la ciberseguridad

Las amenazas a la seguridad pueden llevarse a cabo por una variedad de delincuentes con varias motivaciones diferentes. Al atacar a individuos, los delincuentes buscan conseguir acceso a información y datos personales, usualmente para obtener dinero u otros bienes. El *software* malicioso (*malware*) como los virus o el *software* espía (*spyware*), la suplantación de identidad (*phishing*), y las estafas electrónicas son las amenazas más comunes para los usuarios de Internet. Además, se llevan a cabo ataques más sofisticados para ingresar en complejos sistemas corporativos y gubernamentales con fines de espionaje. De manera similar, se combina una variedad de ciberarmas y ataques para alterar por completo un sistema o una red de terceros.

Las técnicas empleadas para facilitar los tipos de ataques que afectan la confidencialidad, integridad, y disponibilidad de los datos y sistemas son muy diversas y cada vez más sofisticadas.

Software malicioso (malware). El *malware* incluye virus, *spyware*, y otros tipos de *software* no deseados que se instalan en dispositivos digitales sin consentimiento y llevan a cabo tareas indebidas, generalmente para el beneficio del atacante. Estos programas pueden dañar a los dispositivos, y ser usados para robar información personal, monitorear y controlar las actividades en línea, enviar correo no deseado, y cometer fraude, así como también infectar a otros dispositivos de la red. También son capaces de entregar publicidades en línea de carácter indeseado o inapropiado.

Los virus, los caballos de Troya, el *adwar,* y el *spyware* son tipos de *malware*. Un virus se puede replicar a sí mismo y esparcirse hacia otros dispositivos sin que el usuario se dé cuenta. Aunque algunos virus están latentes, la mayoría de ellos están destinados a interferir con los datos o afectar el desempeño de los dispositivos (reformateo del disco rígido, agotamiento de la memoria de la computadora, etc.). Un caballo de Troya es un programa que contiene contenido malicioso o dañino utilizado para abrir una puerta trasera que puedan usar los delincuentes para infiltrar un dispositivo y poner en funcionamiento operaciones remotas adicionales. Los troyanos pueden ser empleados por ciberladrones y hackers que intentan obtener acceso al sistema de un usuario. Generalmente, engañan al usuario mediante algún tipo de ingeniería social para que este descargue o ejecute a los troyanos en su sistema. Una vez activados, los troyanos pueden habilitar a los ciberdelincuentes a espiar a los usuarios, robar datos sensibles, y conseguir acceder por las puertas traseras a sus sistemas.

El *adware* recopila datos comerciales y otra información sin que el usuario lo sepa, o redirige las solicitudes de búsqueda a ciertos sitios web de publicidad. El *spyware* vigila a los usuarios, recopila información sobre ellos, y se la transmite a las partes interesadas sin que el usuario lo note. Los tipos de información recolectada pueden incluir: sitios web visitados, información de búsqueda y el sistema, dirección IP de la computadora, así como también información sensible como direcciones de correo electrónico y contraseñas. Adicionalmente, el *malware* puede provocar el secuestro del navegador, en el que la configuración del navegador del usuario sufre modificaciones sin el conocimiento por parte del usuario. Este *software* puede crear accesos directos en el escritorio, mostrar anuncios en ventanas emergentes, y también reemplazar las páginas de inicio existentes o las páginas de búsqueda por otras páginas.

Botnets. Las botnets son redes de dispositivos secuestrados que llevan a cabo, de manera remota, tareas encomendadas sin el conocimiento de los dueños de los dispositivos. Un dispositivo se convierte en un bot tras ser infectado con un tipo específico de *malware*, que también permite el control de manera remota. Las botnets son utilizadas para realizar una amplia variedad de delitos y ataques: distribución de correos no deseados, esparcimiento de infecciones de *malware* a más dispositivos, colaboración en los fraudes de pago por clic, o usurpación de identidad. Uno de los usos más preocupantes de las botnets es el de llevar a cabo ataques de denegación de servicio (DDoS) distribuidos (Figura 11).

Los investigadores y las compañías de ciberseguridad advirtieron que las botnets se están convirtiendo en la mayor amenaza para la seguridad de Internet, ya que aumentan los efectos de los virus y otros programas maliciosos, incrementan el número de robos de información, y propulsan los ataques DoS. Para ilustrar la dimensión de esta amenaza, la botnet Simda, derribada en abril de 2015, afectó a computadoras en 190 países e involucró el uso de 14 servidores de comando y control en 5 países.[2]

Los ataques DoS inundan una computadora o un sitio web con solicitudes de información, imposibilitando su buen funcionamiento. Estos ataques tienen el propósito de agotar los

Figura 11. Botnet

recursos disponibles en una red, aplicación, o servicio, para evitar que los usuarios accedan a ellos. La mayoría de las veces están dirigidos a empresas, más que a individuos. Los ataques DDoS son los ataques en los que muchas computadoras comprometidas atacan a un solo objetivo.

Un ataque DoS no siempre resulta en el robo de información u otra pérdida en el contexto de la seguridad, pero puede causar pérdidas financieras o de tiempo a la organización o persona afectada, debido a sus efectos (indisponibilidad de algunos servicios de red en particular, cese de operaciones de sitios web, impedimento de la recepción de correos legítimos en las cuentas de correo electrónico a las que se dirigió el ataque, etc.).

Phishing. El *phishing* es una forma de ingeniería social por la cual una persona cae en la trampa de hacer algo que normalmente no debería hacer, como brindar información confidencial (por ejemplo, el nombre de usuario y contraseña), abrir un archivo desconocido, o seguir un enlace poco confiable. Una forma de *phishing* consiste en afirmar falsamente, mediante un correo electrónico, las redes sociales, u otros servicios en línea, que sea una entidad existente y de confianza (como un banco), de modo que el destinatario proporcione información personal o confidencial.

Estafas electrónicas (E-scams). Las estafas electrónicas se refieren a esquemas de fraude en los que los estafadores usan uno o más servicios en línea, como correos electrónicos o sitios web, para contactar a víctimas potenciales con ofertas fraudulentas (a menudo en forma de oportunidades de negocio o de inversión, formas fáciles de ganar dinero, estafas involucrando la salud, o importantes descuentos de compra en línea). Las estafas electrónicas se han asociado comúnmente con el fraude de correo electrónico y, cada vez más, con las redes sociales.

Políticas y reglamentación de la ciberseguridad

Muchas iniciativas nacionales, regionales, y mundiales se centran en la ciberseguridad. A nivel nacional, un creciente volumen de legislación y jurisprudencia aborda a la ciberseguridad, con un énfasis en la lucha contra la ciberdelincuencia, y cada vez más, en la protección de la CII contra el sabotaje y los ataques a causa del terrorismo o los conflictos. Es difícil encontrar un país desarrollado que no posea iniciativa alguna que se enfoque en la ciberseguridad. A nivel regional y global, existen muchas iniciativas y actividades.

Actividades de ciberseguridad globales

Naciones Unidas

La ONU ha estado llevando a cabo debates sobre el asunto de la ciberseguridad desde hace un tiempo. En 1998, la Federación Rusa introdujo una resolución borrador en el Primer Comité de la Asamblea General de la ONU sobre los desarrollos en el campo de la información y las telecomunicaciones en el contexto de la seguridad de la información.[3] Luego, en 2004, se creó el GGE de la ONU con el objetivo de examinar las amenazas existentes y potenciales desde la esfera cibernética y las posibles medidas de cooperación para abordarlas. El mandato del grupo se reconfirmó en 2009, 2011, 2013, y 2015. El principal resultado del reporte del 2013 elaborado por el GGE de la ONU fue la reconfirmación del principio de que las leyes internacionales existentes aplican al uso de las TIC por parte de los estados. Además, el informe de 2015 especifica que el estado no debería llevar a cabo o apoyar a sabiendas una actividad de TIC que dañe intencionalmente o que perjudique el uso y operación de la CI.[4]

La Conferencia de Desarme de la ONU ofrece otro posible campo para el debate de la ciberseguridad a nivel diplomático alto. Hasta ahora, aunque algunos miembros, como China, propusieron agregar la ciberseguridad a la agenda, el grupo no ha podido ponerse de acuerdo con un plan de trabajo.[5]

En el campo de la ciberdelincuencia, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, por sus siglas en inglés) es la organización líder. Algunos documentos jurídicos de la UNODC, como la Convención contra la Delincuencia Organizada Transnacional (UNTOC, por sus siglas en inglés), no se utilizan lo suficiente en la lucha contra la ciberdelincuencia. La mayor parte de la delincuencia cibernética es organizada (cometida por al menos 3 personas) y transfronteriza (organizada en más de un estado e, incluso, organizada por grupos en un estado con efectos sustanciales sobre otro estado).

Unión Internacional de Telecomunicaciones

La UIT fue mandatada por los resultados de la CMSI en 2005 para dar seguimiento a la Línea de Acción C5 de la Agenda de Túnez, titulada Construyendo Confianza y Seguridad en el Uso de las TIC.

La UIT realiza varias actividades relacionadas con la ciberseguridad. Sin embargo, solamente una parte de ese trabajo relacionado con la seguridad de la infraestructura de telecomunicación posee una naturaleza de toma de decisiones (o en realidad, de establecimiento de estándares); gran cantidad de este trabajo tiene que ver con la investigación, la concientización, y el desarrollo de capacidades.

Una de las actividades más visibles es la Agenda sobre ciberseguridad global (GCA, por sus siglas en inglés)[6] de la UIT, lanzada en 2007 por su Secretario General como un marco para la cooperación internacional para mejorar la confianza y la seguridad en la sociedad de la información. La GCA está diseñada para la cooperación y eficiencia, fomentando la colaboración con y entre todas las partes relevantes, y elaborando aun más las iniciativas existentes para evitar la duplicación de esfuerzos. Mediante su asociación con la Alianza Internacional Multilateral contra las Ciberamenazas (IMPACT, por sus siglas en inglés). La UIT también brinda asistencia a los países del mundo para el desarrollo de soluciones y políticas de ciberseguridad. La GCA está construida sobre cinco pilares estratégicos: medidas legales, medidas técnicas y procesales, estructuras organizacionales, desarrollo de capacidades, y cooperación internacional.

Otra actividad de la UIT es el Índice Mundial de Ciberseguridad (IMC), una iniciativa de múltiples partes interesadas destinada a medir el compromiso de los países con la ciberseguridad.[7]

Foro de Gobernanza de Internet

La ciberseguridad ha sido un tema de gran prominencia en la agenda del IGF desde su primera reunión en 2006. Por ejemplo, fue el tema central en una de las sesiones principales y en muchos talleres en la reunión del IGF en João Pessoa en Brasil en noviembre de 2015, con una atención especial sobre la seguridad, el cifrado, y la confianza.[8] En un quinto de los talleres del IGF de 2015 se trataron temas relacionados con la ciberseguridad. En 2016, la ciberseguridad se escogió como el tema del Foro de Mejores Prácticas del IGF, que se centró en el abordaje de la cooperación y colaboración entre los grupos de múltiples actores interesados en el área de la ciberseguridad. Aunque el IGF no toma decisiones ni proporciona recomendaciones, sí brinda la oportunidad de llevar a cabo diálogos y alianzas, intercambiar información, y brindar una guía voluntaria y útil sobre las políticas mediante los Foros de Mejores Prácticas y los informes sobre las sesiones temáticas que se mantienen cada año.

Conferencia Global sobre el Ciberespacio

La Conferencia Global sobre el Ciberespacio (GCCS en inglés) emergió como una serie de conferencias en las que se debatían los principios relativos al «comportamiento rector en el ciberespacio».[9] A veces nos referimos a las conferencias como el Proceso de Londres, ya que la primera de estas tuvo lugar en Londres en 2011. La segunda conferencia fue en Budapest en 2012, luego en Seúl en 2013, y la cuarta se mantuvo en La Haya durante la primavera de 2015.

La GCCS reúne a representantes de gobiernos, incluso muchos ministros, así como también representantes de alto nivel del sector empresarial y la sociedad civil. No elabora conclusiones o tratados formales además de la Declaración del Presidente, pero brinda una importante oportunidad para el debate y la cooperación, así como también una plataforma para las negociaciones sobre posibles acuerdos futuros dentro de otros marcos.

En la GCCS de 2015, se estableció el Foro Global de Experticia Cibernética (GFCE, por sus siglas en inglés) con la intención de compartir experiencias, identificar vacíos, y complementar los esfuerzos existentes en el desarrollo de las capacidades cibernéticas. Los miembros del Foro son: gobiernos, organizaciones internacionales, y compañías privadas. Ellos trabajan conjuntamente con la comunidad técnica, las organizaciones de la sociedad civil, y los académicos, para elaborar iniciativas en el área del desarrollo de las capacidades

cibernéticas. Todos los miembros adoptaron la Declaración de La Haya que enfatiza la necesidad de un mayor desarrollo de las capacidades, más intercambio de mejores prácticas, y una cooperación internacional fortalecida.[10]

OTAN

La OTAN, por ser una organización de defensa colectiva, se concentra en los esfuerzos relacionados con la ciberseguridad sobre la defensa cibernética. La OTAN siguió el ritmo de los rápidos cambios en el panorama de amenazas instigadas por la creciente dependencia hacia la tecnología e Internet, y por lo tanto ha incorporado de manera decisiva la defensa cibernética en su marco estratégico e institucional. Los cambios se produjeron incluso en el marco doctrinario de la organización, ya que los 28 estados miembros acordaron en 2016 incluir al ciberespacio como el cuarto dominio operacional, además del aéreo, terrestre, y marítimo.[11]

La actual política de defensa cibernética de la OTAN, promulgada en 2014, contiene, entre otras cosas, procedimientos para auxiliar a los estados miembros a que definan las maneras de avanzar con las tareas de concientización, educación, capacitación, y ejercicio; y para que pongan de relieve la necesidad de progresar en las iniciativas de cooperación – con países aliados, otras organizaciones internacionales, y también con la industria. Aunque la prioridad máxima de la OTAN en la defensa cibernética es la protección de los sistemas de comunicación e información que pertenecen y son operados por la organización, también depende de una confiable y segura infraestructura nacional de sus países miembros.

El Centro de Excelencia OTAN de Ciberdefensa Cooperativa (CCD CoE, por sus siglas en inglés) lanzó el Manual de Tallín en 2009 «como esfuerzo principal en la investigación y educación del derecho cibernético internacional», que consistió en programas de investigación y capacitación profesional, siendo el Manual de Tallín sobre la Ley Internacional aplicable a la Ciberguerra el documento internacional clave que emite propuestas relacionadas con la aplicación del derecho internacional al ciberespacio.[12] El CCD CoE también desarrolló un exhaustivo Manual sobre el Marco Nacional de Ciberseguridad, que proporciona información de base detallada y marcos teóricos pormenorizados para ayudar en la comprensión de las varias facetas de la ciberseguridad nacional, según los distintos niveles de formulación de políticas públicas. Los cuatro niveles de gobierno – político, estratégico, operacional, y táctico/técnico – tienen sus propios puntos de vista acerca de la ciberseguridad nacional, y cada uno está desarrollado en secciones separadas dentro del Manual. Adicionalmente, el Manual proporciona ejemplos de instituciones importantes en la ciberseguridad nacional, que van desde los órganos de coordinación de políticas de alto nivel hasta estructuras de manejo de cibercrisis e instituciones similares.[13]

Actividades regionales de ciberseguridad

A nivel regional, cada vez más organizaciones están tomando conciencia acerca de la importancia de la ciberseguridad y están desarrollando estrategias, recomendaciones, y convenios, como el Convenio sobre la Ciberdelincuencia del CdE, la Estrategia sobre la Seguridad del Espacio en línea de la Cooperación Económica de Asia Pacífico (APEC, por sus siglas en inglés), la Estrategia de Ciberseguridad de la UE, la Decisión de la OSCE sobre las Medidas para el Fomento de la Confianza, y el Convenio de Ciberseguridad de África.

Europa

Europa fue una de las primeras regiones en abordar la ciberseguridad. El CdE promulgó el Convenio sobre Ciberdelincuencia,[14] que entró en vigencia el 1 de julio de 2004. Este

Convenio inspiró muchas otras reglamentaciones regionales y nacionales sobre la ciberdelincuencia en todo el mundo. Sigue siendo el instrumento jurídico internacional más importante en el campo digital, con la ratificación de los países europeos, y también de EE. UU., Canadá, Japón, y muchos otros países no europeos. Dado que ha sido ratificado por muchos países más allá del continente europeo, se ha debatido la posibilidad de hacer que el Convenio sea un instrumento global sobre la ciberdelincuencia. Sin embargo, algunos países mantienen sus reservas acerca de su entrada al Convenio, por razones que varían desde motivos simbólicos (no haber participado en las negociaciones del documento) hasta sustantivos (por ejemplo, la posibilidad de realizar investigaciones transfronterizas).

A nivel de la UE, la Estrategia de Ciberseguridad y la Directiva sobre la seguridad de la red y los sistemas de información (Directiva NIS) son los dos documentos principales en el área de la ciberseguridad. La Estrategia describe una serie de prioridades y acciones estratégicas destinadas a abordar los desafíos de la seguridad en el ciberespacio, que se concentran en lograr la resiliencia cibernética, reducir considerablemente la ciberdelincuencia, desarrollar políticas y capacidades de ciberdefensa, desarrollar recursos industriales y tecnológicos para la ciberseguridad, y establecer una política coherente internacional sobre el ciberespacio para la UE.[15] La Directiva contiene disposiciones sobre las medidas por implementar a cargo de los estados miembros con el objetivo de lograr un elevado nivel común sobre la ciberseguridad dentro de la UE. Dichas medidas incluyen, entre otras, la adopción de estrategias nacionales para la seguridad de la red y los sistemas de información, la designación de autoridades nacionales competentes y de Equipos de Respuesta frente a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés), y la identificación de operadoras de servicios esenciales sobre las cuales imponer obligaciones para la toma de medidas de seguridad adecuadas.[16]

La OSCE también trabaja para la ciberseguridad, particularmente en las medidas de construcción de confianza (CBM, por sus siglas en inglés). Estas medidas generalmente están diseñadas para colaborar en el mejoramiento de las relaciones entre los estados, llegar a acuerdos pacíficos tras los conflictos, o prevenir el desencadenamiento de una confrontación militar. Son dos las decisiones más notables del Consejo Permanente de la OSCE sobre las CBM que ejemplifican la participación de la OSCE en el ciberespacio. El primer conjunto de CBM de la OSCE de 2013 tiene como fin reducir el riesgo de la aparición de conflictos provenientes del uso de las TIC.[17] Estas medidas voluntarias incluyen compartir opiniones nacionales sobre amenazas y mejores prácticas, cooperar con los órganos nacionales competentes, pedir asesoramiento para reducir los riesgos de percepciones erróneas y posibles tensiones o conflictos, construir una legislación nacional que permita compartir información, y compartir y debatir acerca de la terminología nacional relacionada con la ciberseguridad. En 2016, el segundo conjunto de CBM expandió su cobertura, particularmente hacia las asociaciones público-privadas (PPP en inglés).[18]

Se espera que nuevos conjuntos de CBM se puedan acordar dentro de la OSCE en un futuro cercano. A medida que el éxito de las CBM llega a las comunidades diplomáticas, es probable que las CBM puedan además aportar más al trabajo del GGE de la ONU.

Américas

En 2013, la Organización de las Estados Americanos (OEA) construyó la Estrategia Interamericana de Ciberseguridad[19] que reúne los esfuerzos de tres agrupaciones relacionadas de la organización: el Comité Interamericano contra el Terrorismo (CICTE); Ministros de Justicia y otros Ministros, Procuradores, o Fiscales Generales de las Américas (REMJA en inglés); y la Comisión Interamericana de Telecomunicaciones (CITEL). Estos grupos

trabajan con los estados miembros para implementar programas que prevengan la ciberdelincuencia y para proteger a la CI mediante medidas legislativas y otras medidas procesales. El Grupo de Trabajo sobre Ciberdelincuencia, parte de REMJA, organiza talleres técnicos para fortalecer la capacidad de los estados miembros para desarrollar las medidas legislativas y procesales correspondientes a la ciberdelincuencia y a la evidencia electrónica.[20]

Asia

En Asia, el Foro Regional (ARF) de la Asociación de Naciones del Sudeste Asiático (ASEAN, por sus siglas en inglés) aborda las medidas de fomento de la confianza en la ciberseguridad y lucha contra la ciberdelincuencia. En 2012, el ARF produjo una declaración ministerial destinada a intensificar la cooperación regional en la seguridad de las TIC.[21] En 2013, el ARF puso a la ciberseguridad nuevamente en su agenda, concentrándose en la lucha contra el terrorismo y el crimen transnacional, mientras que la Reunión Ministerial de la ASEAN contra el Crimen Transnacional decidió crear un Grupo de Trabajo sobre Ciberdelincuencia.[22]

La Organización de Cooperación de Shanghái (OCS), que incluye a China, Rusia, y los países de Asia Central, lleva a cabo intensas actividades en el campo de la ciberseguridad. Asumió un acuerdo de cooperación en el campo de la garantía de la seguridad internacional de la información. Además, a finales de 2011, los miembros de la OCS le propusieron a la ONU un Código Internacional de Conducta para la Seguridad de la Información, que se reintrodujo en 2015, en una versión actualizada.[23]

África

En África, la política de ciberseguridad se centró en la elaboración del Convenio de la Unión Africana sobre la Ciberseguridad y la Protección de los Datos Personales.[24] Actualmente, este convenio está en proceso de ratificación. En general, en África, el foco principal está en el desarrollo de las capacidades de instituciones nacionales y regionales que se ocupan de la ciberseguridad.

Actividades bilaterales

Cada vez con mayor frecuencia, los países recurren a vías bilaterales para hacer frente a problemas de ciberseguridad. Varían desde tratados bilaterales mediante acuerdos de coordinación hasta consultas informales. Los Estados Unidos utilizan los Tratados de Asistencia Legal Mutual (MLAT, por sus siglas en inglés), suscrito por más de 20 países, para la colaboración en materia de ciberdelincuencia. Muchos países han firmado acuerdos de cooperación sobre ciberseguridad que especifican el intercambio de información y actividades coordinadas.

Además, los principales actores en ciberseguridad utilizan conversaciones bilaterales para aumentar la cooperación y apaciguar potenciales conflictos. Por ejemplo, China mantiene conversaciones tanto con EE. UU. como con la UE. Australia ha desarrollado conversaciones cibernéticas con China, EE. UU., Corea del Sur, India, y Nueva Zelanda. India y Rusia también establecieron conversaciones sobre ciberseguridad y, en 2016, los dos países concluyeron un acuerdo formal.

Iniciativas técnicas y académicas

Los CERT/CSIRT han representado el principal vehículo para la cooperación técnica en el ámbito de la ciberseguridad. Los CERT cooperan cruzando las fronteras nacionales:

es una cooperación regional. El Foro Internacional de Equipos de Respuesta a Incidentes y Seguridad (FIRST, por sus siglas en inglés) coordina una red internacional técnica de CERT nacionales.

Iniciativas empresariales

Un creciente número de iniciativas para la mejora de la seguridad proviene del sector empresarial, especialmente de los fabricantes de *software* y *hardware* más grandes. Su participación en el marco general de política internacional se ve motivada, por un lado, por la necesidad de introducir mejoras tecnológicas junto con las normativas, y, por el otro, por sus propios intereses empresariales en el aumento de la confianza de los usuarios finales en la tecnología.

Microsoft ha propuesto un conjunto de normas de ciberseguridad para reducir los conflictos en el ciberespacio,[25] lo que representó la primera iniciativa de este estilo por parte de un actor empresarial en el campo de la paz internacional, que comúnmente es el ámbito de los diplomáticos y los estados. En cooperación con la Asociación sobre Investigación de Delitos de Alta Tecnología (HTCIA, por sus siglas en inglés), Microsoft lanzó un Portal para la Comunidad sobre Delitos Digitales, portal al que los organismos de aplicación de la ley tienen acceso, para ayudarlos con las investigaciones sobre la ciberdelincuencia.

Cisco ha desarrollado una gama de certificaciones de seguridad de la red para los profesionales y organizaciones de TI.

Los departamentos de investigación externa y de relaciones universitarias dentro de compañías multinacionales de *software* y *hardware* en todo el mundo, incluidas Microsoft, SAP, Cisco, y otras, se dedican a construir fuertes relaciones con las principales universidades, organismos gubernamentales, organizaciones profesionales, y socios de la industria, para profundizar la investigación, mejorar la experiencia de enseñanza y aprendizaje, y promover la innovación tecnológica. La cooperación se realiza mediante una variedad de programas: trabajo de investigación conjunto por parte de instituciones académicas y ramas de investigación local de estas compañías; subvenciones para la investigación; apoyo a las conferencias; becas para doctorados; y otros trabajos con universidades, instituciones, y escuelas para distribuir un plan de estudios innovador.

Principales desafíos en el abordaje de asuntos de ciberseguridad

Confusión terminológica en el campo de la ciberseguridad

Las políticas públicas de Internet son un campo político en formación. Por lo tanto, existe aún gran confusión terminológica, que varía desde diferencias benignas como el uso indistinto de palabras o afijos (ciber/electrónico/digital/net/virtual) hasta diferencias esenciales, cuando el uso de términos diferentes refleja distintos enfoques políticos. En el área de la ciberseguridad, el potencial de confusión es significativo, y comienza por el mero nombre utilizado para describir este campo político. China, Rusia, y los países de la OCS usan el término «seguridad de la información», que es más amplio, ya que cubre también la estabilidad política y social. Ellos consideran que la ciberseguridad es solamente una subcategoría técnica de la seguridad de la información. Para EE. UU., la UE, y los países de la OCDE, la ciberseguridad es un término general que se concentra principalmente en la protección de la infraestructura de Internet. Para estos países, la seguridad de la información es una subcategoría de la ciberseguridad que aborda, más que nada, datos e información.

También existen diferencias en la manera en que varios actores entienden conceptos como la CII, las ciberarmas, y el ciberterrorismo. Abordar esta confusión terminológica es extremadamente importante. La comunidad internacional necesitaría contar con mucho tiempo y atravesar prolongadas negociaciones para llegar a un entendimiento común sobre la ciberseguridad. Lamentablemente, los riesgos que suponen los malos entendidos son inmediatos y no deberían ser subestimados. Un primer paso podría ser identificar las diferentes terminologías y trazar sus coberturas semánticas. Tras este primer paso de identificación de diferencias, debería ser posible identificar las posibles convergencias y desarrollar gradualmente un vocabulario sobre ciberseguridad en común.

Enfoque multidisciplinario hacia la ciberseguridad

La ciberseguridad no puede abordarse de manera separada a otros aspectos de la política digital como los derechos humanos y el desarrollo económico, tal como lo muestra el triángulo de políticas en la Figura 12.[26]

Una respuesta sistemática significativa para los riesgos a la ciberseguridad depende, por lo tanto, de un profundo entendimiento de los aspectos multidisciplinarios del ciberespacio: el nexo entre la tecnología, el derecho, la psicología, la sociología, la economía, la ciencia política, y la diplomacia. La eficiencia de dicha respuesta depende además de las sociedades entre los múltiples actores interesados que pueden contribuir a la reducción de los riesgos.

- Las autoridades gubernamentales y normativas, con sus habilidades para crear un entorno jurídico, reglamentario, y normativo para la ciberseguridad.

- Las instituciones judiciales y las autoridades de aplicación de la ley, con sus competencias y responsabilidades de persecución penal y mecanismos de cooperación transfronterizos.

Figura 12. Triángulo de la política de la ciberseguridad

- El sector privado y las comunidades técnicas, con su experticia y control *de facto* sobre la mayor parte de la infraestructura, y la mayoría de los servicios y estándares.

- Las ONG y el sector académico con sus conocimientos, redes, y capacidad para llegar a los usuarios finales y advertirles sobre el uso indebido del ciberespacio.

La arquitectura técnica de Internet y la ciberseguridad

La propia naturaleza de Internet y su organización afecta a su seguridad. ¿Deberíamos continuar con el enfoque actual que se basa en construir la seguridad sobre los cimientos preexistentes e inseguros, o modificar las bases de la infraestructura de Internet? ¿Cómo afectarían dichas modificaciones a otras características de Internet, especialmente su apertura y transparencia? La mayoría de los desarrollos anteriores de los estándares de Internet tenían la intención de mejorar el desempeño o introducir nuevas aplicaciones. La seguridad no era una de las prioridades. No queda claro si la IETF será capaz de cambiar los estándares de correos electrónicos para brindar una autenticación adecuada y, a futuro, reducir el uso indebido de Internet (por ejemplo, el correo no deseado y la ciberdelincuencia).

Dada la controversia que rodea a los cambios en los estándares básicos de Internet, es probable que las mejoras en cuanto a la privacidad en el protocolo básico de Internet se introduzcan de manera gradual y lentamente. No obstante, se están comenzando a tomar pasos importantes en esta dirección; las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC en inglés)[27] es un buen ejemplo ilustrativo. Tras casi 12 años de investigación, pruebas, y debates dentro de la comunidad técnica, las DNSSEC se utilizaron por primera vez para algunos ccTLD, y a partir de 2010 también se implementaron a nivel de los servidores raíz. Sin embargo, quedan más desafíos por enfrentar en el camino hacia la implementación a gran escala de este nuevo estándar de seguridad por parte de los registradores de nombres de dominio, los PSI, y los propietarios de sitios web.

Sin embargo, se pueden lograr mejoras importantes en la seguridad mediante la correcta configuración de los principales nodos de Internet como los servidores DNS alrededor del mundo. Muchos incidentes, como la ciberguerra privada de 2013 entre dos compañías – CyberBunker y Spamhaus – que resultó en la congestión temporaria de grandes porciones de la Internet mundial, son posibles debido a varias docenas de millones de servidores DNS alrededor del mundo mal configurados, conocidos como resolutores abiertos.[28] Además, la introducción de la seguridad por diseño en todas las nuevas tecnologías – *software, hardware,* y protocolos – traería capas de seguridad adicionales, que podrían representar fortificaciones y bloqueos.

Ciberseguridad, confianza, y comercio electrónico

La ciberseguridad a menudo aparece en la lista de los requisitos previos para el rápido crecimiento del comercio electrónico. Sin una Internet segura y confiable, la confianza se verá disminuida, y los usuarios de Internet se mostrarán reacios a proporcionar información confidencial en línea, como los números de tarjetas de crédito. Similar es el caso del banco en línea (*online banking)* y el uso de dinero electrónico. Estamos presenciando un creciente número de ataques exitosos a los servidores de compañías para obtener los datos personales y los números de las tarjetas de crédito de los consumidores, como la recopilación de más de 1,2 mil millones de combinaciones de nombre de usuario y contraseña, y 500 millones de direcciones de correo electrónico robadas en 2014 por un grupo de rusia.[29] Estos incidentes socavan la confianza del usuario en los servicios en línea. Si la ciberseguridad

en general solamente mejora a paso lento (y con una falta de estándares), es probable que el sector empresarial exija desarrollos más rápidos en la ciberseguridad. Esto puede resultar en más desafíos para el principio de la neutralidad de la red y el desarrollo de «una nueva Internet», que facilitaría, entre otras cosas, una comunicación en Internet más segura.

Vigilancia y espionaje

Las revelaciones de 2013 del empleado de la NSA, Edward Snowden, confirmaron que los estados – incluido EE. UU. – explotan las vulnerabilidades de Internet para sus propios intereses. El proyecto de metodología de la NSA para el registro de información personal (que se conoce como PRISM, por sus siglas en inglés) basó sus capacidades de vigilancia en la habilidad de acceder a cables, enrutadores, y servidores de la nube de las principales compañías de Internet (empresas de telecomunicaciones, proveedores de servicios y contenido con sede en EE. UU.). Ante esto, otros países – especialmente los de la UE y los países BRIC (Brasil, Rusia, India, China, y Sudáfrica) – comenzaron a tener en consideración tácticas paliativas, que incluían colocar sus propias conexiones intercontinentales por cables submarinos,[30] y solicitar a las compañías de Internet que almacenen los datos personales de sus ciudadanos en centros de datos dentro de sus jurisdicciones.

Ciberespionaje económico

En 2013, la compañía de seguridad Mandiant, con sede en EE. UU., publicó un informe sobre ataques de ciberespionaje originadas desde China, contra compañías de EE. UU.[31] Luego de que EE. UU. acusara a cinco «hackers militares» chinos, por su parte, China acusó a EE. UU. de ciberespionaje. Todo esto resultó en la suspensión de las actividades del Grupo de Trabajo Cibernético Chino-Estadounidense.[32] Esta crisis llegó a su pico máximo antes de la visita del presidente chino Xi Jinping a EE. UU. en septiembre de 2015, momento en el que el gobierno estadounidense amenazó con sancionar a China debido al ciberespionaje económico. Durante esta visita, los dos países acordaron no apoyar a sabiendas el ciberespionaje contra el sector empresarial.[33] Esta regla (en proceso de formación) contra el ciberespionaje económico recibió apoyo adicional en la Cumbre del G-20 en Antalya (15-16 de noviembre de 2015), en la que los países del G-20 coincidieron en que «ningún país debe conducir o apoyar el robo de propiedad intelectual a través de ITCs, incluidos los secretos comerciales u otra información confidencial de negocios, con la intención de proporcionar ventajas competitivas a las empresas o sectores comerciales».[34]

El aumento de la militarización del ciberespacio mediante el uso de vulnerabilidades y herramientas de hackeo por parte de los estados está provocando una creciente tensión política. Esta tensión puede agilizar la necesidad de que existan esfuerzos globales para prevenir la proliferación de ciberarmas.

Ciberseguridad y derechos humanos

El vínculo entre la ciberseguridad y los derechos humanos es extremadamente importante para el futuro de la Internet. Hasta el momento, estas dos áreas se han abordado por separado en sus respectivos silos. Sin embargo, experiencias recientes (SOPA, ACTA PRISM/NSA) muestran que la protección de los derechos humanos (privacidad, libertad de expresión, acceso) no es solo una prioridad basada en valores, sino también una herramienta muy útil para garantizar que la Internet permanezca abierta y segura.

Los usuarios de Internet individuales representan los pilares de la ciberseguridad. Aun así, a menudo son el eslabón más débil cuando se trata de la protección contra los ciberataques.

Nuestras computadoras personales son el escenario en el que se montan los ciberataques (como partes de botnets) y esparcen virus y *malware*. El acceso desprotegido a nuestras computadoras y dispositivos móviles ofrece una puerta trasera de acceso a los conjuntos de datos de nuestras compañías o instituciones, y compromete a muchas más computadoras.

No obstante, las preocupaciones de los usuarios finales, por lo general, no son sobre el posible daño mayor (a menudo debido a la ignorancia) como resultado de sus computadoras comprometidas, sino sobre la protección de sus propios datos, y por lo tanto, la integridad y privacidad en general. Los debates tras las revelaciones sobre PRISM se centran en lograr que las computadoras personales sean más «seguras en lo que respecta a la vigilancia», lo que incluye el empleo del cifrado, periódicos parches y actualizaciones, IPSec (seguridad del Protocolo de Internet), y VPN[35] – medidas de concientización que, de hecho, también evitarían el acceso desprotegido y contribuirían a una mejor ciberseguridad general.

Una de las piedras angulares de la ciberseguridad global – construida en torno al importante rol de los usuarios de Internet individuales – son los derechos humanos. El reconocimiento de este nexo ya ha comenzado a aparecer en los documentos de políticas. La Estrategia de Ciberseguridad de la UE, por ejemplo, considera que la preservación de un ciberespacio abierto, libre, y seguro – incluido el apoyo para la promoción y protección de los derechos fundamentales – es uno de los cinco pilares de la estrategia.

La ciberseguridad y la privacidad se representan a menudo como una compensación entre sí en un equilibrio, como se puede ver en la Figura 13. Esto no siempre es así.

El principal reto es apuntar a soluciones ganadoras/ganadoras: una mayor seguridad implica más derechos humanos y viceversa. De hecho, hay muchas áreas ganadoras/ganadoras en el empoderamiento y la protección de los individuos como pilares del sistema de seguridad cibernética (acceso a la información, protección de la privacidad), a las que se debe dar prioridad. En última instancia, los derechos humanos son una cuestión de realpolitik de ciberseguridad.

www.igbook.info/cybersecurity

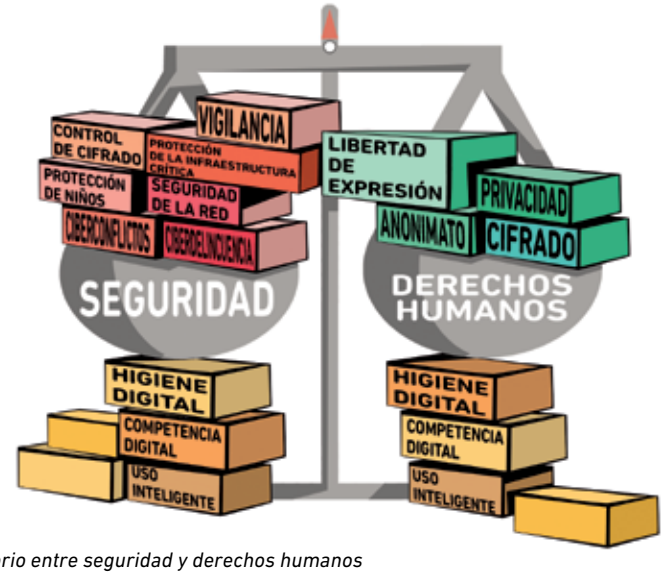

Figura 13. Equilibrio entre seguridad y derechos humanos

Ciberdelincuencia

Existe una dicotomía entre el derecho real y el ciberderecho en el debate sobre la ciberdelincuencia. El enfoque del derecho real subraya que la ciberdelincuencia es igual que el crimen fuera de línea, pero que se comete con el uso de herramientas digitales. El delito es el mismo; solo cambian las herramientas. El enfoque del ciberderecho hace hincapié en que los elementos únicos de la ciberdelincuencia justifican un tratamiento especial, más que nada cuando se trata de la aplicación de la ley y la prevención.

Los redactores del Convenio sobre ciberdelincuencia del CdE se acercaron más al enfoque del derecho real, resaltando que el único aspecto específico de la ciberdelincuencia es el uso de las TIC como los medios para cometer el crimen. El convenio, que entró en vigor el 1 de julio de 2004, es el principal documento internacional en este campo.

La prominencia de la ciberdelincuencia la colocó en la agenda de varias organizaciones internacionales, regionales, y locales, debido a la continua incidencia y diversificación de los crímenes cometidos en relación con los sistemas de redes electrónicas o mediante su uso.[36] Un ejemplo es la Iniciativa contra la Ciberdelincuencia de la Commonwealth,[37] que nació en el marco del Foro de Gobernanza de Internet de la Commonwealth (CIGF, por sus siglas en inglés). El sector comercial también reconoció la importancia de la lucha contra la ciberdelincuencia y ha comenzado iniciativas privadas para apoyar campañas de concientización y la mejora de las disposiciones legales.

Los asuntos

Definición de ciberdelincuencia

La ciberdelincuencia se define como los delitos cometidos mediante Internet y sistemas informáticos. Uno de los tipos de ciberdelitos es el que afecta la confidencialidad, integridad, y disponibilidad de los datos y sistemas informáticos. Incluyen el acceso no autorizado a sistemas informáticos, la interceptación de la transmisión de datos, la interferencia de datos (daño, eliminación, deterioro, alteración, o supresión de datos), la interferencia de sistemas (la obstaculización sin derecho del funcionamiento de una computadora u otro dispositivo), la falsificación, el fraude, y la usurpación de identidad. Otros tipos de ciberdelitos son los relacionados con el contenido, y tienen que ver con la producción, oferta, distribución, adjudicación, y posesión de contenido en línea que se considere ilegal según las leyes nacionales: contenido en línea de abuso sexual infantil, contenido que promueva un acto terrorista, contenido extremista (incitación al odio, la violencia, o actos de terrorismo), ciberacoso (comportamiento ofensivo, amenazante, o acosador mediante el uso de la tecnología).

Ciberdelincuencia y la protección de derechos humanos

El Convenio sobre la Ciberdelincuencia cristalizó el debate acerca del equilibrio entre la seguridad y los derechos humanos. Los actores de la sociedad civil expresaron su preocupación acerca de que el Convenio les confiere a las autoridades del estado un poder muy amplio, que incluye el derecho a revisar computadoras personales, y llevar a cabo la vigilancia de las comunicaciones, entre otras cosas. Estos amplios poderes tienen el potencial de poner en peligro los derechos humanos, particularmente la privacidad y la libertad de expresión.[38] El hecho de que el CdE – con quien se deposita el Convenio – promueva de

manera activa los derechos humanos puede ayudar a lograr el equilibrio necesario entre la lucha contra la ciberdelincuencia y la protección de los derechos humanos. En este contexto, cabe mencionar que el Comité de Ministros del Consejo adoptó, en 2014, una Recomendación para los estados miembros sobre una Guía de los derechos humanos de los usuarios de Internet, que explica, entre otras disposiciones, que «nadie deberá estar sujeto a injerencias ilícitas, innecesarias o desproporcionadas en el ejercicio de sus derechos humanos y sus libertades fundamentales al usar Internet».[39]

Recopilación y preservación de pruebas

Uno de los principales desafíos en la lucha contra la ciberdelincuencia es la recopilación de pruebas para los procesos judiciales. La velocidad de las comunicaciones de hoy en día exige una rápida respuesta por parte de las agencias de aplicación de la ley. Una posibilidad para preservar las pruebas se encuentra en los registros de red, que brindan información sobre quién accedió a determinados recursos de Internet y cuándo. El Convenio sobre la Ciberdelincuencia impone específicamente la obligación preservar los datos de tráfico de Internet.

Bajo la creciente presión de las amenazas y los ataques terroristas cibernéticos, la UE dio otro paso hacia adelante y aprobó la Directiva sobre la Conservación de Datos, que exigía que los PSI conservaran los datos de tráfico y ubicación «con fines de investigación, detección y enjuiciamiento de delitos graves [...], definidos por cada Estado miembro en su ordenamiento jurídico interno».[40] Esta disposición recibió fuertes críticas por motivos de privacidad, y sucedió que varios estados no consiguieron promulgar una legislación nacional para cumplir con esta directiva o bien anularon dichas leyes declarándolas inconstitucionales.[41] En diciembre de 2013, el TJEU declaró que la Directiva sobre la Conservación de Datos era incompatible con la Carta de los Derechos Fundamentales.[42]

www.igbook.info/cybercrime

Infraestructura crítica

Según la Comisión Europea, la CI consiste en «instalaciones, redes, servicios, y equipos físicos y de tecnología de la información» cuya interrupción o destrucción podría poner en peligro «la salud, la seguridad, o el bienestar económico de los ciudadanos, o el eficaz funcionamiento de los gobiernos de los Estados miembros».[43] Algunos ejemplos de estas infraestructuras incluyen aquellas que se dedican al funcionamiento de los servicios de energía, transporte, suministro de agua, comunicación, finanzas, y salud. Los países definen sus propias CI dependiendo de su contexto nacional; si bien la mayoría de los países desarrollados han dado el paso de definir sus CI, no sucede lo mismo con la mayoría de los países en vías de desarrollo.

La CI depende cada vez más de los sistemas de control basados en el código digital (como los sistemas de control industrial del control de supervisión y adquisición de datos (SCADA, por sus siglas en inglés) y están conectados mediante redes basadas en IP (una Intrarred, o, a menudo, redes virtuales privadas mediante la Internet pública). Si bien permite la optimización de recursos, esto también pone a la CI ante el riesgo de ciberataques. Estos ataques pueden ser ataques DDoS (Figura 14), control remoto de sistemas industriales, recopilación de información sensible, o interrupción del funcionamiento normal de las instalaciones

mediante el cambio de los parámetros de control y comando – como fue el caso con el virus Stuxnet, o durante el ciberataque a una fábrica de acero alemana a fines de 2014. [44]

Protección de la infraestructura crítica (de información)

Una subcategoría específica de la CI es la CII. El Glosario de Seguridad de la IETF define a la CII como «sistemas que son tan vitales para una nación que su incapacidad o destrucción tendría un efecto debilitante sobre la seguridad nacional, la economía, o la salud y la seguridad pública».[45]

La protección de la CII hace referencia a las reglas, estrategias, planes, y procedimientos que abordan la prevención, preparación, respuesta, y recuperación de desastres y emergencias. Por lo general, se emplean muchas estrategias en conjunción para la protección de la CI. Estas estrategias se ocupan de aspectos como la aplicación de la ley y la prevención del crimen, la lucha contra el terrorismo, la seguridad y defensa nacional, la gestión de emergencias, la planificación de la continuidad empresarial, seguridad y protección, la seguridad electrónica, la planificación y preparación ante desastres naturales, la gestión de riesgos, las redes profesionales, la regulación del mercado, la planificación y el desarrollo de la infraestructura, y la resiliencia organizacional.

En EE. UU., la Directiva Presidencial (PPD21) sobre la Seguridad y Resiliencia de la Infraestructura Crítica[46] de 2013 cubre tanto los sistemas físicos como los virtuales. En la UE, el Programa Europeo de Protección de Infraestructuras Vitales (EPCIP, por sus siglas en inglés)[47] y la Directiva sobre la identificación y designación de infraestructuras críticas europeas[48] se centran en el sector de las TIC como elemento clave. La Directiva de la UE sobre la seguridad de las redes y sistemas de información, junto con la Estrategia de Ciberseguridad de la UE, establecen una guía más específica para los estados miembros sobre las medidas de la protección de las CII (CIIP), que incluyen la creación de CERT. Al

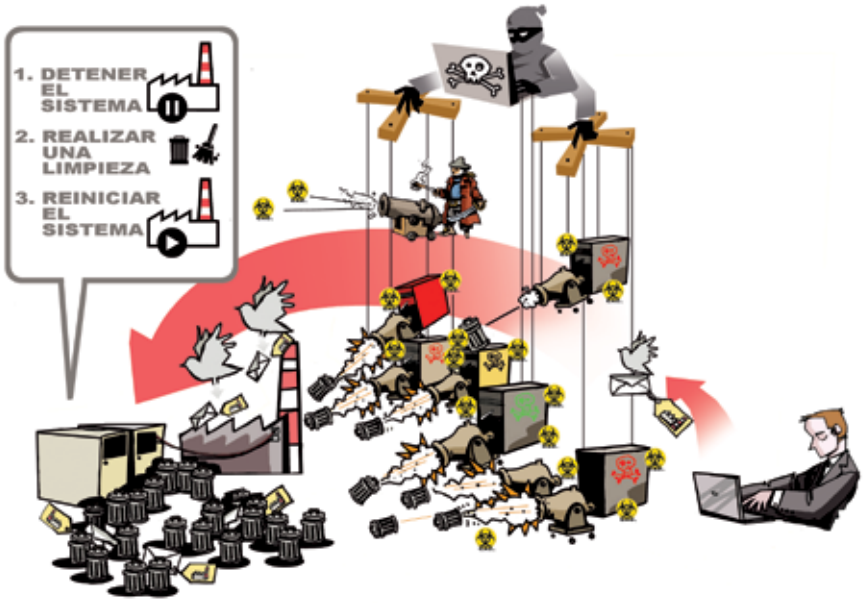

Figura 14. Ataque DDos a la infraestructura crítica

mismo tiempo, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, por sus siglas en inglés) de la UE está a cargo de llevar a cabo el seguimiento de la implementación de medidas para la CIIP, y de proporcionar medidas y recursos para la construcción de capacidad.

La Recomendación de la OCDE del Consejo sobre la protección de las infraestructuras críticas de información[49] describe varios pasos que podrían dar los estados miembros para proteger sus CII: a nivel nacional, se ruega que los estados, entre otras cosas, desarrollen estrategias nacionales; identifiquen agencias y organizaciones gubernamentales a cargo de la CIIP; desarrollen estructuras organizacionales de prevención y respuesta, incluidos los CERT independientes; y dialoguen con el sector privado para la construcción de asociaciones público-privadas confiables. A nivel internacional, se motiva a los estados a mejorar el intercambio de información y fortalecer la cooperación entre instituciones a cargo de la CIIP.

ww.igbook.info/critical

Ciberterrorismo

Existen varias definiciones para el término «ciberterrorismo». Muchos simplemente aplicaron la definición de «terrorismo» al mundo virtual. Hay países, como el Reino Unido, que definen al terrorismo, pero no cuentan con una definición jurídica para «ciberterrorismo».[50] Desde la comunidad académica, una definición – un poco limitada – indica que el ciberterrorismo es el «uso de la tecnología y los medios de información por parte de grupos y agentes terroristas».[51] Una definición más completa y amplia señala que el ciberterrorismo comprende «ataques ilícitos y amenazas de ataques contra computadoras, redes, y la información almacenada en ellas con fines de intimidar o ejercer coacción sobre un gobierno o sus ciudadanos para llevar a cabo objetivos políticos o sociales».[52]

En la práctica, se entiende que el ciberterrorismo incluye uno o más de los siguientes tres aspectos:

- Uso de Internet para llevar a cabo ataques por parte de grupos terroristas (ataques DoS, ataques de hackeo).
- Uso de Internet para la preparación y organización de ataques terroristas.
- Uso de Internet para la promoción de causas terroristas y el reclutamiento de terroristas.

Lucha contra la distribución de la propagada terrorista y el contenido extremista violento en línea

La distribución en línea de la propaganda terrorista y el contenido extremista violento se ha vuelto un tema recurrente en la política internacional, así como también un motivo de preocupación para las compañías de Internet.

Debido a que los terroristas se han vuelto cada vez más sofisticados en el uso de las redes sociales, y a que estas plataformas en línea pueden llegar a más y más gente alrededor del

mundo, la amenaza de la radicalización en línea por parte de los terroristas se ha vuelto el centro de atención de muchos en el área de la toma de decisiones. En abril de 2016, los ministros de relaciones exteriores de China, India y Rusia hicieron una declaración conjunta resaltando la necesidad de luchar contra el aumento de contenido terrorista en línea.[53] Este tema también llegó hasta el Consejo de Seguridad de la ONU, que mantuvo un debate abierto sobre la lucha contra las narrativas e ideologías terroristas.[54] Luego, en mayo de 2016, los líderes del G7 abordaron con más profundidad el tema[55] en Japón.

Además de las discusiones a nivel político, esto también se convirtió en una preocupación para el sector privado, sobre todo para la industria de Internet. En mayo de 2016, Microsoft publicó sus políticas relacionadas con el contenido terrorista en línea, ya que siente que es «una responsabilidad... no contribuir, ni siquiera de modo indirecto, con actos terribles».[56] La incubadora tecnológica de Google, Jigsaw, ha estado experimentando con videos de YouTube modificando los algoritmos de motor de búsqueda de manera tal que las búsquedas en línea de propaganda terrorista pudieran redirigir al usuario hacia contenido antiterrorista.[57]

El funcionamiento práctico de las campañas contra el extremismo necesita estar cuidadosamente equilibrado con el derecho a la libertad de expresión. Hay una delgada línea entre la protección de la seguridad y la promoción de la censura en línea, y la ubicación de esta línea divisoria está bastante abierta a la interpretación. David Kaye, Relator Especial de la ONU sobre la Libertad de Expresión, destacó esta preocupación, y afirmó que el «extremismo violento» podía ser usado como la «excusa perfecta» de los gobiernos para restringir la libertad de expresión.[58] La fórmula adecuada para una política de contenido que asegure el máximo nivel posible de libertad de expresión y, al mismo tiempo, reduzca la radicalización al mínimo, solo se podrá encontrar tras un diálogo continuo entre las comunidades de seguridad y derechos humanos.

Iniciativas para combatir el ciberterrorismo

La falta de consenso sobre la definición de ciberterrorismo puede llevar a la mala interpretación y podría causar un impacto en la cooperación para mitigar las amenazas e incidencias en una escala global. Pero, a pesar de esto, los países están comenzando a tomarse en serio la amenaza del ciberterrorismo. En 2012, se informó que el Departamento de Defensa de los Estados Unidos aceptaba las propuestas para el desarrollo de *software* para predecir «sucesos de ciberterrorismo» detectando la manera en que interactúan los grupos delictivos y los hackers en Internet.[59] El Proyecto Clean IT, liderado por el Ministerio de Seguridad y Justicia holandés entre 2011 y 2013, estaba destinado a «entablar un diálogo constructivo entre gobiernos, empresas, y la sociedad civil para explorar cómo reducir el uso terrorista de Internet». Esto dio como resultado un conjunto de principios generales y una revisión de mejores prácticas.[60]

La ONU le ha estado prestando cada vez más atención al ciberterrorismo. En septiembre de 2006, la Asamblea General de la ONU aprobó la Estrategia Global de las Naciones Unidas contra el Terrorismo,[61] mediante la cual los estados miembros se comprometieron, entre otras cosas, a coordinar sus esfuerzos a nivel internacional y regional para luchar contra el terrorismo en todas sus formas y manifestaciones en Internet. Consecuentemente, se creó un Grupo de Trabajo sobre la lucha contra el uso de Internet con fines terroristas dentro del Equipo Especial para la Ejecución de la Lucha contra el Terrorismo, con la tarea de coordinar las actividades del sistema de las Naciones Unidas para la aplicación de la estrategia.

En 2012, el Grupo de Trabajo, en cooperación con la UNODC, emitió un informe que explora las prácticas y marcos jurídicos existentes a nivel nacional e internacional en relación con la criminalización, investigación, y enjuiciamiento de los casos terroristas relativos a Internet, y proporciona una serie de recomendaciones para los estados en miras de mejorar su cooperación en este campo. [62] El Comité contra el Terrorismo del Consejo de Seguridad de la ONU también ha estado tomando en consideración los aspectos y problemas que emanan del uso de Internet con fines terroristas. En diciembre de 2015, mantuvo una reunión con los estados miembros de la ONU, compañías de Internet, y organizaciones de la sociedad civil, para evitar que los terroristas saquen provecho de Internet y las redes sociales para reclutar terroristas e incitar a cometer actos de terrorismo, y, al mismo tiempo, para respetar los derechos humanos y libertades fundamentales. Las recomendaciones se hicieron durante la reunión sobre la manera en que los estados y el sector privado podrían prevenir y combatir el uso del ciberespacio con fines terroristas, y a su vez, cumplir con los documentos internacionales sobre derechos humanos.[63]

www.igbook.info/cybercrime

Ciberconflicto y ciberguerra

El derecho internacional establecido regula la conducta del conflicto armado tradicional y busca limitar sus efectos. Si bien hay un consenso más sólido acerca de que los marcos jurídicos internacionales ya instaurados también aplican al conflicto en línea, no queda claro cómo se aplican en la práctica.

Un desafío adicional es el de la falta de entendimiento común sobre qué constituye un acto de guerra en el ciberespacio. Una posible definición sugiere que la ciberguerra comprende «acciones de un estado nacional para entrar a las computadoras de otra nación con el propósito de causar daño o alteraciones».[64] Aun así, no existe un acuerdo con respecto a las definiciones, especialmente entre los poderes mundiales cruciales.

Una de las principales características de los ciberataques es que son casi imposibles de atribuir a delincuentes determinados, y mucho menos a los estados, debido al empleo de armas complejas y sofisticadas que se abren camino a través de varias capas proxy (incluidas las botnets). Además, a diferencia de la guerra tradicional, los ciberconflictos no se dan entre dos naciones mientras los demás países observan silenciosamente. La Internet es un recurso global, y las ciberarmas, como las botnets, emplean los recursos informáticos de otras naciones sin su consentimiento. Esto hace que la ciberguerra sea realmente de carácter global.

El hito que abrió los numerosos debates políticos sobre el ciberconflicto y la ciberguerra fueron los ataques a escala nacional por los que atravesó Estonia en abril de 2007. Estonia sufrió ataques DDoS en la infraestructura de Internet, los ministerios de relaciones exteriores y defensa, los principales periódicos, y bancos.[65] Aunque la evidencia circunstancial señaló conexiones entre los ataques y la oposición de Rusia a la reubicación de un monumento a los soldados soviéticos en Tallin, no había pruebas claras de la participación de funcionarios rusos en los ataques. Un caso que se relaciona generalmente con la ciberguerra es el de los ataques a los medios en línea y los servidores gubernamentales georgianos, durante el conflicto entre Rusia y Georgia en 2008. Se conoció al caso como «guerra cibernética»,[66] aunque no hubo pruebas de un ataque promovido por el estado de Rusia.

Los gobiernos de EE. UU. y de Israel llegaron a las noticias por su supuesta participación en los ciberataques a sistemas informáticos que operaban en las principales instalaciones de enriquecimiento nuclear de Irán, lo que destapó el uso sistemático de ciberarmas.[67] Irán, a su vez, había sido acusado de montar ataques en bancos y compañías estadounidenses en represalia por las acciones previas de EE. UU.[68] Las acusaciones del gobierno de EE. UU. acerca de que Corea del Norte había hackeado a Sony a finales de 2014 fueron más lejos cuando EE. UU. introdujo sanciones económicas.[69]

También se dejaron ver enfoques más sutiles con respecto a la ciberguerra. Estados Unidos ha acusado a China de lanzar sistemáticamente actividades de ciberespionaje en contra del gobierno y las infraestructuras de información empresarial (como Google y Microsoft), cosa que China niega.[70] En 2014, cuando los reportes de la compañía de seguridad establecida en los Estados Unidos, Mandiant, revelaron detalles sobre el aumento de los intentos de ciberespionaje de China, este país respondió que también él mismo era víctima, y vinculó estas contraacusaciones con un programa de vigilancia de PRISM que Snowden había develado, y advirtió también que estos incidentes estaban poniendo en peligro la cooperación chino-estadounidense.[71]

Ciberataques en la «guerra híbrida»

Como resultado de la Conferencia de Seguridad de Múnich de 2015, los ciberataques son considerados un segmento importante de la guerra híbrida.[72] Hace referencia a operaciones cibernéticas en tiempos de paz destinadas a dañar la estabilidad y crecimiento del enemigo sin desatar una guerra real.

El empleo de botnets y poderosos armamentos similares basados en Internet en conflictos y ataques transfronterizos tiene el mismo objetivo que la guerra tradicional: ganar los

Figura 15. Armas cibernéticas

recursos económicos de otro territorio o destruir los recursos enemigos. Las ciberarmas pueden estar dirigidas a los sistemas de control de infraestructuras críticas como redes eléctricas, redes de control de tráfico aéreo, o sistemas de seguridad de plantas de energía nuclear (Figura 15).

Un rasgo característico de los ciberataques es que son una manera rentable de atacar a enemigos. Por ejemplo, las investigaciones demuestran que la inversión en instalaciones DDoS robustas y poderosas que podrían llevar a cabo un ataque DDoS a escala nacional puede no superar unos cuantos miles de euros, mientras que el daño económico que causaría un ataque así variaría entre €10 millones por día para un país en transición como Serbia y hasta más de 500 millones de euros por día para un país desarrollado como Suiza.[73] Por lo tanto, las ciberarmas pueden conferir un poder adicional a actores con recursos limitados.

Las ciberarmas pueden utilizarse principalmente como un complemento de las operaciones convencionales, en lugar de un medio independiente para librar una guerra.

www.igbook.info/cyberconflict

Cifrado

El cifrado hace referencia a la codificación de documentos y comunicación en un formato ilegible al que se puede acceder después de la decodificación. Tradicionalmente, los gobiernos eran los únicos actores que tenían el poder y el conocimiento para desarrollar y emplear un cifrado poderoso en sus comunicaciones militares y diplomáticas. El cifrado se volvió asequible para los usuarios de Internet con aplicaciones como Pretty Good Privacy. Recientemente, ha habido muchas plataformas que ofrecen protección para las comunicaciones mediante el cifrado, incluidas Silent Circle, Telegraph, y Proton. Además, las compañías de Internet han empezado a usar un poderoso cifrado para la protección de sus comunicaciones internas y los datos de los usuarios.

Debido a que el cifrado se está volviendo más asequible para básicamente todos los usuarios de Internet, incluidos los criminales y terroristas, el posible uso indebido de las herramientas de cifrado ha abierto uno de los debates clave sobre políticas digitales en todo el mundo entre gobiernos y empresas. El centro de este debate está en lograr el equilibrio justo entre la necesidad de respetar la privacidad de la comunicaciones de los usuarios de Internet y la necesidad de que los gobiernos monitoreen algunos tipos de comunicaciones de relevancia para la seguridad nacional (las posibles actividades delictivas y terroristas siguen siendo un problema).

Aplicaciones principales

Muy a menudo, percibimos al cifrado como una herramienta para proteger la confidencialidad de las comunicaciones. Por un lado, deberíamos cifrar el contenido almacenado en nuestra computadora o en la nube mediante el uso de herramientas de cifrado, o pedir a nuestro operador de servicios en la nube que cifre nuestro contenido en sus servidores. Por otro lado, también deberíamos cifrar el contenido durante su recorrido desde nuestra computadora a su destino (ya sea un sitio web de una red social o la bandeja de entrada de un amigo). Debido a que el proceso de cifrado requiere de tiempo y capacidades informáticas,

es probable que no sea la configuración por defecto de muchos proveedores públicos de servicios en la nube o de comunicaciones, dada la masa de datos que necesitarían cifrar, a menudo en tiempo real. Aun así, cada vez una mayor cantidad de compañías entiende que el cifrado es una oferta opcional que puede satisfacer las exigencias de los clientes, lo que aumentaría también su competitividad; el caso de Apple y WhatsApp marca la tendencia. También existen varias soluciones de *software* disponibles, y que a menudo son libres, para el anonimato en línea que están basadas en el cifrado, como la red Tor (un *software* de código abierto que fue desarrollado para proteger la privacidad y las libertades fundamentales mediante el anonimato y el impedimento del análisis de tráfico y la vigilancia).

El cifrado es un componente crucial también para la seguridad adicional de los protocolos de Internet clave. El IPSec, las DNSSEC, y el Protocolo de Seguridad Border Gateway (BGPSec) están basados en la distribución de certificados digitales para que los servidores y enrutadores sean capaces de verificar la identidad de los números IP, nombres de dominio, y rutas escogidas, y de evitar el *spoofing* y la suplantación de identidad por servidores falsos. De manera similar, la SSL (capa de puertos seguros) establece un enlace cifrado entre un servidor web y un buscador, asegurando que la comunicación entre estos permanezca secreta y completa.

Cifrado y estandarización

El avance del poder informático hace posible un cifrado más rápido, pero también un análisis criptográfico acelerado, lo que hace que los estándares cambien con más regularidad. A la decisión sobre cuáles son los algoritmos más sofisticados que podrían convertirse en estándares *de facto* para ser implementados en productos comerciales la toman los ingenieros y científicos dentro de sus organizaciones, como la IETF; organizaciones privadas sin fines de lucro que abordan los estándares, como el Instituto Nacional Americano de Estándares; y los órganos de estandarización nacionales de los estados más poderosos económicamente (que pueden invertir en la criptografía), como el Instituto Nacional de Normas y Tecnología de EE. UU. Debido al creciente interés geopolítico en la vigilancia de Internet, confrontado por una variedad de tendencias para el cifrado de uso masivo, los servicios de seguridad nacional comenzaron a mostrar más interés en los procesos de estandarización liderados por científicos: tras las revelaciones de Snowden, *Der Spiegel* informó que los «agentes de la NSA viajan a las reuniones de la IETF, una organización que desarrolla estos estándares, para recopilar información pero, al parecer, también para influenciar los debates que se mantienen allí».[74]

Regímenes internacionales para las herramientas de cifrado

Los aspectos internacionales de la política de cifrado implican la coordinación a nivel de seguridad y de la empresa privada.

Por ejemplo, la política de EE. UU. para el control de la exportación de *software* de cifrado no fue muy exitosa porque no podía controlar la distribución internacional. Las compañías de *software* de EE. UU. iniciaron una fuerte campaña de presión argumentando que los controles de exportación no aumentan la seguridad nacional, sino que socavan los intereses empresariales de EE. UU.

El cifrado se ha abordado en dos contextos: el Acuerdo de Wassenaar y la OCDE. El Acuerdo de Wassenaar es un régimen internacional adoptado por 41 países para restringir

la exportación de armas convencionales y tecnologías de doble uso a países en guerra o países que son considerados «estados parias».[75] El acuerdo estableció una secretaría en Viena. La presión de EE. UU., con el Grupo de Wassenaar, quería extender el Enfoque Clipper[76] internacionalmente, mediante el control del *software* de cifrado a través de un depósito de claves. Muchos países se resistieron, especialmente Japón y los países nórdicos.

Se llegó a un acuerdo en 1998 mediante la introducción de directrices sobre criptografía, que incluían una lista de control de doble uso de productos de *software* y *hardware* de criptografía de más de 56 bits. Esta extensión incluía herramientas de Internet, como buscadores web y correo electrónico. Cabe señalar que este arreglo no cubre transferencias «intangibles», como la descarga. La imposibilidad de introducir una versión internacional del Clipper contribuyó a dejar de lado esta propuesta de manera nacional en EE. UU. En este ejemplo del lazo entre los campos nacionales e internacionales, los desarrollos internacionales tuvieron un impacto decisivo sobre los nacionales.

La OCDE es otro foro para la cooperación internacional en el campo del cifrado. Aunque la OCDE no produce documentos legalmente vinculantes, sus lineamientos sobre varios asuntos son altamente respetables. Son el resultado de un enfoque experto y un proceso de toma de decisiones basado en consensos. La mayoría de sus directrices, tarde o temprano, se incorporan a las legislaciones nacionales. El cifrado fue un tema muy controvertido en las actividades de la OCDE. Inició en 1996 con la propuesta de EE. UU. de adoptar un depósito de claves como estándar internacional. Al igual que con Wassenaar, las negociaciones de la propuesta estadounidense de adoptar un depósito de claves con estándares internacionales sufrieron fuertes oposiciones por parte de Japón y los países nórdicos. El resultado fue una especificación acordada de los principales elementos políticos del cifrado.

Algunos intentos por desarrollar un régimen internacional para el cifrado, principalmente en el marco del Acuerdo de Wassenaar, no resultaron en el desarrollo de un régimen internacional efectivo. Aún es posible conseguir un poderoso *software* de cifrado en Internet.

Seguridad y derechos humanos

La encriptación faculta a los ciudadanos para proteger su privacidad. El cifrado también es utilizado por criminales y terroristas para proteger sus comunicaciones. Se están volviendo cada vez más habilidosos en el uso de Internet para el apoyo de la logística, como la adquisición de armas mediante Internet, como fue el caso de los atentados terroristas en París en 2015.[77] El uso de servidores proxy anónimos disponibles públicamente y la anonimización de los servicios como Tor para acceder a la *dark web* (web oscura), junto con la transferencia de dinero por medio de una moneda criptográfica como Bitcoin, deja muy pocos rastros y hace que la vigilancia en línea y el análisis forense digital sean altamente complejos. Además, los dispositivos móviles cada vez más seguros, con tecnología de cifrado de vanguardia, como iPhone o Silent Circle, y una variedad de aplicaciones móviles para los chats cifrados como Telegram y Signal – a pesar de que protegen a los informantes y a los activistas de oposición de todo el mundo – también proporciona un entorno seguro para la coordinación interna de grupos terroristas, evitando la interceptación de las comunicaciones.

Como respuesta, los gobiernos y servicios de seguridad de muchos países, incluidos el Reino Unido, Francia, y EE. UU., están intentando introducir límites a la fuerza de los algoritmos de cifrado dentro de productos y servicios convencionales, y crear mecanismos que permitirían a las agencias gubernamentales acceder a datos cifrados en caso de que

fuera necesario. Además, algunos países, como EE. UU., el Reino Unido, y Rusia, han estado realizando tareas para introducir legislación específica que exigiría que las compañías tecnológicas permitan que las agencias de aplicación de la ley accedan a los datos/servicios cifrados (en circunstancias más o menos determinadas), o que las ayuden a acceder a dichos datos. Los gobiernos argumentan que el acceso a los datos cifrados tiene una creciente importancia para las acciones destinadas a prevenir y enjuiciar delitos graves, y asegurar la seguridad pública.

Las comunidades de la sociedad civil y de derechos humanos han expresado sus fuertes preocupaciones sobre estos desarrollos, además exacerbados por las revelaciones de Snowden. Sugierieron también que dichos métodos podrían ser utilizados para la censura política y la vigilancia desproporcionada (masiva), que a su vez podrían comprometer la identidad de activistas políticos, bloggers, y periodistas, en estados autoritarios, lo que pondría en riesgo su seguridad individual. Además, ha habido estudios que afirman que puede que el cifrado no proteja a los delincuentes tanto como tienden a alegar las agencias de aplicación de la ley,[78] y que la introducción de puertas traseras obligatorias en productos cifrados no sería efectiva.[79]

Desde el punto de vista de los derechos humanos, el derecho a la privacidad y otros derechos humanos deberían estar protegidos, y las herramientas de cifrado – incluso el cifrado ubicuo – son esenciales para resguardar la privacidad. El informe del Relator Especial para el CDH de la ONU sobre el uso del cifrado y el anonimato para el ejercicio de los derechos de libertad de opinión y de expresión en la era digital destacó la necesidad de contar con una mayor protección para el cifrado y el anonimato. [80]

Los aspectos del cifrado de seguridad y los derechos humanos se han debatido extensivamente a nivel internacional, especialmente tras el altamente publicitado caso Apple-FBI, que recibió mucha atención durante el primer semestre de 2016. El caso, en el que una orden judicial solicitaba que Apple ayudara al FBI a desbloquear un iPhone, disparó dos puntos de vista opuestos: Por un lado, Apple, respaldada por otras compañías de Internet, y también activistas de derechos humanos, argumentó que cumplir con esa solicitud crearía un peligroso precedente y socavaría gravemente la privacidad y seguridad de sus usuarios. Por el otro, las autoridades afirman que el caso no comprendía puertas traseras ni descifrado, sino que era una solución «excepcional», necesaria para el caso; también acusaron a Apple de conferir más valor a sus intereses empresariales que a la investigación del terrorismo. Si bien el caso fue desechado eventualmente (ya que el Departamento de Justicia de EE. UU. anunció que fue capaz de desbloquear el iPhone con la ayuda de un tercero), surgieron preguntas que todavía quedan sin responder. Por un lado, ¿bajo qué circunstancias las autoridades están facultadas para solicitar a las compañías tecnológicas que violen la seguridad de sus sistemas creados para sus dispositivos? ¿Cuáles son, o deberían ser, las salvaguardas establecidas? ¿Debería permitirse que las autoridades influencien la manera en que las compañías diseñan sus productos? Y por otro lado, ¿hasta qué punto las compañías deben proteger la privacidad de sus usuarios? ¿Deberían proteger la privacidad cueste lo que cueste?[81]

Existe una tensión cada vez mayor entre la industria de Internet, que intenta recuperar la confianza que se perdió tras las revelaciones de Snowden, mediante la introducción de fuerte cifrado por defecto, y los servicios de seguridad e inteligencia, que están buscando la manera de inspeccionar las comunicaciones digitales, para finalmente ponerle un fin al desarrollo e implementación abiertos de las herramientas de cifrado. Las autoridades, ¿deberían tener el derecho de explorar las vulnerabilidades que existen en los sistemas comerciales? ¿Bajo qué circunstancias? ¿Deberían estar obligadas a divulgar las vulnerabilidades identificadas al público o a un proveedor, para brindar la posibilidad de reparación del servicio?

Mientras que estas preguntas y muchas otras permanecen sin respuesta, muchas compañías de Internet y tecnología continúan implementando el cifrado en sus productos y servicios, y buscando soluciones para hacer que el cifrado de estos productos y servicios sea inquebrantable incluso para sus fabricantes (lo que haría obsoleta cualquier solicitud gubernamental para la asistencia en la violación de mecanismos de cifrado o en el acceso de datos cifrados).

www.igbook.info/encryption

Correo no deseado

La situación actual

El correo no deseado es correo electrónico no solicitado enviado a un gran número de usuarios de Internet. Generalmente, el correo no deseado se usa con fines de promoción comercial. Otros de sus usos incluyen el activismo social, las campañas políticas, la distribución de contenido pornográfico, y, cada vez con mayor frecuencia, la distribución de *malware*. Además de que es molesto, el correo no deseado generalmente también causa una pérdida económica considerable, tanto en términos del ancho de banda utilizado como la pérdida de tiempo mientras lo revisamos/eliminamos, pero también por el contenido de *malware* que se entrega cada vez más mediante el correo no deseado (y que a menudo resulta en el robo de detalles de cuentas bancarias e información económicamente sensible).[82]

Aunque hace 10 años el correo no deseado era uno de los problemas clave para la gobernanza de Internet, actualmente cuenta con menos prominencia gracias a los filtros tecnológicos altamente sofisticados. Según las estadísticas de 2015, el correo no deseado representó un 54% del total del correo electrónico entrante, comparado con el 84,9% en 2010.[83] Sin embargo, los investigadores advierten que, si bien el nivel de correo no deseado en el tráfico de los correos electrónicos ha disminuido de manera constante en los últimos años, la cantidad de correos electrónicos con contenido malicioso se ha incrementado significativamente (Figura 16). Por ejemplo, Kaspersky Lab notó que el número de correos no deseados con contenido malicioso enviado durante el primer trimestre de 2016 fue 3,3 veces mayor que durante el mismo periodo de 2015.[84] A modo de ejemplo, el «famoso» ransomware troyano Locky, que se identificó por primera vez en febrero de 2016, se ha propagado alrededor del mundo mediante mensajes de correo electrónico no deseados; los informes de abril de 2016 mostraron que se llevaron a cabo intentos por infectar a usuarios con este troyano en más de 110 países.[85]

El correo no deseado puede combatirse mediante medios técnicos y legales. Desde el aspecto técnico, están disponibles muchas aplicaciones para el filtrado de mensajes y la detección de correo no deseado. La comunidad técnica ha desarrollado muchas mejores prácticas, incluidas las del Grupo de Trabajo Anti-Abuso vía Mensajería, Malware y Móviles (M3AAWG en inglés), el Proyecto Spamhaus, la GSMA, y la Internet Society.

La respuesta legal

Los métodos técnicos para combatir el correo no deseado solamente tienen un efecto limitado y necesitan medidas legales complementarias. Desde la parte legal, muchos estados reaccionaron mediante la introducción de nuevas leyes en contra del correo no deseado. En EE. UU., la Ley Can-Spam establece un delicado equilibrio entre la posibilidad de la promoción

vía correo electrónico y la prevención del correo no deseado.[86] Aunque la ley dispone penas severas como resultado de la distribución de correo no deseado, incluso penas de privación de la libertad de hasta cinco años,[87] algunas de sus disposiciones, según los críticos, toleran y hasta incentivan la actividad relacionada con el envío de correo no deseado. La posición inicial por defecto estipulada en la ley es que se permite el correo no deseado hasta que el receptor de los mensajes no deseados dice «basta» (haciendo uso de la cláusula *opt-out*).

En julio de 2003, la UE introdujo su propia ley contra el correo no deseado como parte de su Directiva sobre privacidad y comunicaciones electrónicas.[88] La ley de la UE prevé que, como regla general, el envío de correos electrónicos para el marketing directo puede permitirse siempre y cuando los usuarios hayan dado su consentimiento previo (el enfoque *opt-in*). Sin embargo, hay excepciones en el caso de las relaciones empresariales o comerciales preexistentes: el uso de detalles de contacto electrónico para el marketing directo puede permitirse si se les da a los usuarios la oportunidad de oponerse a esto ya sea en el momento de la recopilación de los datos, o en las etapas siguientes (el enfoque *opt-out*). La directiva también fomenta la autorregulación y las iniciativas del sector privado que causarían una reducción en la cantidad de correos no deseados.

Ambas leyes contra el correo no deseado promulgadas por EE. UU. y la UE tienen un punto débil: carecen de una disposición que prevenga el correo no deseado transfronterizo. Se llegó a una conclusión similar en un estudio sobre la ley contra el correo no deseado de la UE elaborado por el Instituto del Derecho de la Información de la Universidad de Ámsterdam: «El simple hecho de que la mayoría de los correos no deseados se originan fuera de la UE restringe la efectividad de la Directiva de la Unión Europea de una manera significativa».[89] Se necesita una solución global, implementada mediante un tratado internacional o algún mecanismo similar.

Un memorándum de entendimiento (MoU, por sus siglas en inglés) firmado en 2013 por Australia, Corea, y el Reino Unido es uno de los primeros ejemplos de la cooperación internacional en la campaña contra los correos no deseados. El memorándum incentiva

Figura 16. Correo no deseado (Spam)

la cooperación en la reducción de correos no deseados que se originan en cada país y se envían a los usuarios finales en cada uno de ellos. Más recientemente, en junio de 2016, se firmó otro MoU entre las autoridades de Canadá, EE. UU., Australia, los Países Bajos, Corea, Nueva Zelanda, y Sudáfrica.[90]

La OCDE estableció una fuerza de trabajo sobre los correos no deseados y preparó un conjunto de herramientas en su contra. La UIT también ha estado llevando a cabo una serie de actividades destinadas a combatir el correo no deseado. El RTI contiene disposiciones sobre la prevención de «comunicaciones electrónicas masivas no solicitadas», que, algunos interpretan, incluye al correo electrónico no deseado. Sin embargo, estas disposiciones no contienen un lenguaje vinculante; en cambio, simplemente señalan que los países «deben esforzarse para tomar las medidas necesarias» y los alienta a cooperar entre sí.

Consulte la Sección 4 para conocer más sobre el RTI.

De manera similar, una resolución de la Asamblea Mundial de Normalización de las Telecomunicaciones (WTSA, por sus siglas en inglés) de la UIT en 2012 insta a los estados a dar los pasos necesarios para combatir el correo no deseado, y hace referencia solamente a los marcos nacionales.[91] Desde la práctica, la UIT, mediante su Sector de Normalización de las Telecomunicaciones (UIT-T) trabaja para identificar las modalidades adecuadas para combatir el correo no deseado; por ejemplo, la Comisión de Estudio 17 – Seguridad del UIT-T realiza estudios sobre las potenciales medidas para combatir el correo no deseado, y trabaja en el desarrollo de recomendaciones técnicas para cubrir nuevas formas de correo no deseado. Los aspectos que aborda la Comisión incluyen formas de correo no deseado en las redes actuales y futuras, los efectos del correo no deseado, tecnologías que empoderan la creación y la distribución de correo no deseado, y las soluciones para combatirlo. A nivel regional, la APEC ha elaborado un conjunto de Principios para la Acción contra el Spam,[92] y la Unión Africana (UA) incorporó disposiciones sobre la «publicidad a través de medios electrónicos» (incluido el correo electrónico) en el Convenio de la Unión Africana sobre la Ciberseguridad y la Protección de Datos Personales.[93]

Otra iniciativa dedicada a la lucha contra el correo no deseado es el Plan de Acción de Londres, que funciona como marco para la cooperación internacional en la aplicación de la legislación relacionada con el correo electrónico no deseado y en el abordaje de desafíos similares como el fraude en línea, el *malware*, *phishing,* y la diseminación de virus. La red, establecida en 2004, reúne a las autoridades de regulación de más de 25 países, así como también a representantes de la comunidad técnica y el sector comercial.

Los asuntos

Sistemas de filtrado

Existen varios asuntos relacionados con el correo no deseado. Desde la perspectiva técnica, uno de los principales problemas con los sistemas de filtrado es que también se conoce que eliminan correos que sí son deseados. Por ejemplo, el filtrado de correo no deseado de Verizon llegó a los tribunales porque también bloqueaba mensajes legítimos, lo que causó problemas para los usuarios que no recibían sus correos electrónicos legítimos. Sin embargo, la industria contra el correo no deseado está en crecimiento, desarrollando cada vez más aplicaciones sofisticadas capaces de distinguir el correo no deseado del correo normal.

Diferentes definiciones de «correo no deseado»

Las distintas interpretaciones del concepto afectan la campaña en su contra. En EE. UU., la preocupación general acerca de la protección de la libertad de expresión y la Primera Enmienda afectan también a esta campaña. Los legisladores de EE. UU. consideran que el correo no deseado es solamente «correo electrónico comercial no solicitado», dejando afuera otros tipos de correo no deseado, como el activismo político y la pornografía. En la mayoría de los demás países, se considera que el correo no deseado es cualquier «correo electrónico en masa no solicitado», sin importar su contenido. Debido a que la mayoría de los correos no deseados tienen su origen en EE. UU.,[94] esta diferencia en las definiciones limita gravemente la posibilidad de introducir un mecanismo internacional efectivo contra el correo no deseado.

El correo no deseado y la autenticación de correo electrónico

Una de los habilitadores estructurales para el correo no deseado es la posibilidad de enviar mensajes de correo electrónico con una dirección de remitente falsa. Existe una posible solución técnica para este problema, para la cual se deberían hacer cambios en los estándares existentes sobre correo electrónico de Internet. La IETF ha tomado en consideración dichos cambios para el protocolo de correo electrónico, que asegurarían la autenticación de direcciones de correo. Este es un ejemplo de cómo los asuntos técnicos (los estándares) pueden afectar a las políticas. Un posible sacrificio que podría causar la introducción de la autenticación de correo electrónico es la restricción del anonimato en Internet.

La necesidad de tomar medidas globales

La mayoría de los correos no deseados proviene desde fuera de un determinado país. Por lo tanto, es un problema global que requiere una solución global. Existen varias iniciativas que podrían llevar a una cooperación mundial mejorada. Algunas de ellas, como los MoU bilaterales o multilaterales, ya fueron mencionadas. Otras medidas incluyen la construcción de la capacidad y el intercambio de información. Una solución más completa sería elaborar algún tipo de instrumento global contra el correo no deseado. Hasta ahora, los países desarrollados prefieren el fortalecimiento de las medidas nacionales junto con campañas bilaterales o regionales contra el correo no deseado. Dado que están en una situación de desventaja de recibir un «mal público global» que se origina más que nada en los países desarrollados, la mayoría de los que están en vías de desarrollo muestra interés en moldear una respuesta global para el problema de los correos no deseados.

www.igbook.info/spam

Firmas digitales

En términos generales, las firmas digitales[95] están ligadas a la autenticación de individuos en Internet, y son importantes en las áreas de jurisdicción, ciberdelincuencia, y comercio exterior. El uso de firmas digitales debería contribuir a la construcción de confianza en Internet. La autenticación digital en general es, a menudo, considerada una parte del marco del comercio electrónico, ya que tiene la finalidad de facilitar las transacciones de comercio electrónico mediante la celebración de contratos electrónicos. Por ejemplo, ¿se considera válido y vinculante un acuerdo que se completa vía correo electrónico o mediante un sitio web? En muchos países, la ley exige que los contratos estén «escritos

en papel» o «firmados». ¿Qué significa esto para la Internet? ¿Cómo se puede verificar la integridad de un documento firmado electrónicamente? Frente a estos dilemas y bajo la presión de establecer un entorno que habilite el comercio electrónico, muchos gobiernos comenzaron a promulgar legislaciones sobre firmas digitales.

Cuando se trata de firmas digitales, el desafío principal es que los gobiernos no están regulando un problema existente, como la ciberdelincuencia o la violación de derechos de autor, sino que están creando un nuevo entorno normativo para un desarrollo que es relativamente nuevo. Esto condujo a una variedad de soluciones en las disposiciones sobre la firma digital. Surgieron tres grandes enfoques para la regulación de las firmas digitales:[96]

El primer enfoque es minimalista. Especifica que las firmas electrónicas no pueden denegarse porque están en un soporte electrónico. Este enfoque estipula un uso muy amplio de las firmas digitales y fue adoptado en países de *common law*: EE. UU., Canadá, Nueva Zelanda, y Australia.

El segundo Enfoque es maximalista, y señala el marco y los procedimientos para la firma digital, incluidos la criptografía y el uso de los identificadores de clave pública. Este enfoque usualmente plantea el establecimiento de autoridades de certificación dedicadas, que puedan certificar a los futuros usuarios de firmas digitales. Este enfoque ha prevalecido en las leyes de los países europeos, como Alemania e Italia.

El tercer enfoque es una combinación de los dos anteriores. Tiene una disposición minimalista para el reconocimiento de firmas a través de un medio electrónico. El enfoque maximalista también es reconocido mediante la concesión de que las «formas electrónicas avanzadas» tendrán un efecto jurídico más fuerte en el sistema legal (por ejemplo, será más fácil corroborar estas firmas en casos judiciales). La UE adoptó este enfoque en su Directiva sobre la Firma Electrónica y su modificatoria, el Reglamento de identificación electrónica y servicios de confianza digitales para las transacciones electrónicas en el mercado interior (el Reglamento eIDAS).[97] El Reglamento de la UE redefine el concepto de firmas electrónicas avanzadas, introduce los servicios de confianza digitales, y asegura un marco jurídico unificado para la UE.

A nivel mundial, en 2001, la Comisión de las Naciones Unidas para el derecho mercantil internacional (UNCITRAL, por sus siglas en inglés) aprobó la Ley Modelo sobre las Firmas Electrónicas,[98] que les confiere el mismo estatus de las firmas escritas a mano a las firmas digitales, siempre y cuando se cumplan ciertos requisitos técnicos.

Las iniciativas de la infraestructura de clave pública (PKI, por sus siglas en inglés) están directamente relacionadas con las firmas digitales. Dos organizaciones, la UIT y la IETF, están involucradas en la estandarización de la PKI.

Los asuntos

Autenticación de usuarios

Las firmas digitales son parte de una consideración más amplia de la relación entre la privacidad y la autenticación en Internet. Son solamente una de las técnicas importantes utilizadas para la identificación de individuos en Internet.[99] Por ejemplo, en algunos países en los que la legislación sobre la firma digital o sus estándares y procedimientos todavía no han sido establecidos, los bancos utilizan la autenticación SMS por medio de teléfonos móviles para aprobar las transacciones en línea de sus clientes.

La necesidad de detallar la implementación de los estándares

Aunque muchos países desarrollados adoptaron una amplia legislación sobre la firma digital, esta a menudo carece de detalles de implementación de estándares y procedimientos. Debido al carácter novedoso de estos asuntos, muchos países están esperando ver en qué dirección se desarrollarán los estándares concretos. Las iniciativas de estandarización se dan en muchos niveles, incluso en organizaciones internacionales, (UIT e ISO), órganos regionales (el Comité Europeo de Normalización [CEN], ETSI, órganos locales (como el Instituto Nacional de Normas y Tecnología de EE. UU.), y asociaciones profesionales (la IETF).

Neutralidad tecnológica

La implementación de nuevos tipos de firmas electrónicas, como los datos biométricos, va en aumento en muchos países. Como en muchos otros ámbitos, especialmente aquellos en los que la tecnología y la innovación evolucionan a pasos agigantados, los legisladores necesitan lograr un equilibrio entre la codificación de estos mecanismos, y al mismo tiempo legislar de una manera tecnológicamente neutral para evitar el riesgo de que se vuelva obsoleta rápidamente.

El riesgo de la incompatibilidad

La variedad de enfoques y estándares en el ámbito de las firmas digitales podría llevar a la incompatibilidad entre diferentes sistemas nacionales. Las soluciones mosaico podrían restringir el desarrollo del comercio electrónico a nivel mundial. Los órganos regionales y locales deberían lograr la armonización necesaria.

www.igbook.info/esignature

Seguridad infantil en línea

Los niños están usando Internet cada vez más. Esto trae beneficios a los niños y jóvenes,[100] como oportunidades para su educación, el desarrollo personal, la expresión personal, y la interacción con otras personas. Al mismo tiempo, también presenta riesgos a los que los niños y jóvenes son especialmente vulnerables.

Cuando se trata de promover los beneficios de la tecnología para los niños y al mismo tiempo fomentar un entorno en línea seguro y protegido, las partes interesadas necesitan lograr un equilibrio justo: por un lado, los niños deben quedar protegidos contra el contenido inapropiado y el comportamiento peligroso; por el otro, deben respetar sus derechos de acceso a la información y libertad de expresión, entre otros.

Consulte la Sección 8 para saber más sobre los derechos digitales de los niños.

Los desafíos

Comprender la manera en que los niños usan la tecnología y la Internet es esencial para la elaboración de políticas e iniciativas relacionadas con la seguridad infantil en línea. El

entorno evoluciona rápidamente y está en constante producción de nueva tecnología que tiene un impacto significativo en las vidas de los niños y su seguridad. Aunque no existe un único esquema aplicable universalmente a la protección de los niños en línea, sus actitudes y el uso de la tecnología moldea los procesos de elaboración de políticas y moviliza a la acción a las partes interesadas.

Riesgos para los niños en línea

A pesar de los numerosos beneficios de Internet, los niños y jóvenes se enfrentan a riesgos en línea al usar la Internet y la tecnología. Si bien los usuarios de cualquier edad también enfrentan riesgos, los niños son particularmente vulnerables, ya que todavía se encuentran en su etapa de desarrollo. Sobre la base de varias tipologías,[101] podemos resumir que los riesgos incluyen:

Contenido inapropiado. Los niños pueden quedar expuestos a contenido que es inapropiado debido a sus edades, como el contenido para adultos y material violento. Los juegos violentos, por ejemplo, se están volviendo rápidamente más prominentes que las películas violentas «pasivas», y a menudo contienen armas sofisticadas que muestran características de armas reales, y derramamientos de sangre.

Contacto inapropiado. Los niños pueden quedar expuestos a contenido dañino, como la intimidación y el acoso, y son particularmente propensos a este tipo de contacto al usar herramientas de comunicación en línea como las redes sociales. Si bien los niños generalmente son víctimas de sus propios pares, el contacto inapropiado puede incluir un contacto más peligroso, como la captación de menores cometida por posibles acosadores sexuales.

Conducta inapropiada. Los niños y jóvenes generalmente no consiguen comprender del todo las consecuencias que pueden sufrir ellos mismos y terceros debido a sus «huellas en el mundo digital» a largo plazo. La conducta inapropiada incluye la publicación de comentarios indebidos, o la revelación de información o imágenes personales sensibles que pueden acarrear consecuencias negativas. El *sexting*, o el intercambio de contenido sexual predominantemente a través de la tecnología móvil, es una práctica cada vez más común, e investigaciones han demostrado que los jóvenes sienten cada vez más presión por involucrarse en esta práctica.

Problemas relacionados con los consumidores. También conocidos como «riesgos comerciales», los problemas relacionados con los consumidores incluyen ser el blanco o el receptor de publicidad inapropiada, quedar expuesto a costos ocultos (como las aplicaciones que invitan a los usuarios a adquirir un servicio) y la recepción de correo no deseado. Los niños también enfrentan riesgos relativos a la privacidad en línea y la recopilación de datos, incluidos los datos de geolocalización.

A pesar del amplio rango de riesgos, investigaciones realizadas en Europa sugieren[102] que si bien los niños y jóvenes están más expuestos a los riesgos, no todos los riesgos conducen a un daño real. Mucho depende de la edad, el sexo, y la resiliencia y recursos del niño para enfrentar los riesgos. Los padres, tutores, educadores, el gobierno, el sector comercial, y otras partes interesadas cumplen un rol muy importante en la protección de los niños en línea, y en ayudarlos a lidiar con los riesgos de una forma adecuada.

Abuso y explotación sexual infantil en línea

A pesar de que el problema del abuso sexual infantil no es nuevo, la Internet lo ha exacerbado. Los pervertidos a menudo pueden explorar sus inclinaciones bajo el anonimato, y encontrar maneras de evadir la aplicación de la ley. Algunos de los riesgos en línea

descriptos en este libro pueden terminar en violencia sexual de un tipo u otro: los niños pueden quedar expuestos a los depravados, lo que puede resultar en la captación de menores y la explotación sexual; también pueden convertirse en perpetradores, como cuando se los persuade para crear y compartir imágenes sexuales de ellos mismos, que después pueden ser usadas para acosarlos o amenazarlos.

Al usar redes sociales – que los abusadores usan con frecuencia – los niños y jóvenes no son conscientes de los peligros y las identidades ocultas. La identidad encubierta es uno de los métodos más frecuentemente utilizados por los abusadores en Internet, en donde la conducta virtual se puede transformar en conducta real, aumentando el riesgo de abuso y explotación de menores, la pedofilia, la solicitación de menores con propósitos sexuales, e incluso el tráfico infantil.

Las imágenes de abuso sexual de menores – conocidas comúnmente como «pornografía infantil» en la legislación[103] – son típicamente la representación digital de un abuso sexual en el mundo real. Las investigaciones muestran que las víctimas del contenido de abuso sexual infantil en línea son muy jóvenes, y el abuso es violento e inhumano.

Aunque hay que reconocer que es difícil determinar la cantidad de contenido de abuso sexual infantil que se comparte en línea, la mayor parte de este contenido se encuentra en la *deep web*, donde el contenido no surge normalmente mediante el uso de motores de búsqueda. Debido a que muchos de los delincuentes se vuelven más astutos con respecto a la seguridad y obtienen un conocimiento técnico profundo, la Darknet se está volviendo cada vez más popular entre los depravados y pedófilos.

Casi todo el contenido de abuso infantil que circula abiertamente en Internet es contenido viejo que recircula; el contenido nuevo generalmente representa una nueva víctima. Cuando se descubre contenido que muestra en línea el abuso sexual infligido a un niño, hay dos prioridades claras: eliminar el contenido para que ya no esté disponible al público, y encontrar a la víctima del abuso. Así, se puede quitar a la víctima de ese entorno dañino y ofrecerle el apoyo apropiado.

Abordar los desafíos

Cuando se trata de riesgos en línea, se puede utilizar un enfoque que combine las políticas y legislación adecuada (que incluya la legislación, la auto- y la corregulación, u otras medidas políticas), así como también las herramientas técnicas, educación, y concientización, para abordar los riesgos de una manera amplia.

Medidas normativas

Desde el punto de vista normativo, muchos países han promulgado leyes que califican de ilegal cierto contenido, aunque las definiciones e interpretaciones puedan variar de un país a otro. A nivel internacional, los instrumentos clave son la Convención de las Naciones Unidas sobre los Derechos del Niño y el Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía; el Convenio sobre la Ciberdelincuencia del CdE y el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual (también conocido como el Convenio de Lanzarote). El Centro Internacional para Niños Desaparecidos y Explotados (ICMEC, por sus siglas en inglés) desarrolló su marco para evaluar la legislación nacional, y lo usa regularmente en la legislación en distintos países.

Medidas de auto- y corregulación

La autorregulación (el acuerdo voluntario por parte de la industria) y la corregulación (una combinación entre la regulación gubernamental y la privada) demostraron ser enfoques efectivos, especialmente por parte de la industria. Por ejemplo, los PSI pueden, de manera voluntaria, contemplar medidas de detección y eliminación, y pueden también filtrar ciertos tipos de contenido ilegal; las plataformas de redes sociales pueden establecer un requisito de edad mínima para los niños. También es importante que exista una buena relación laboral entre la industria y la aplicación de la ley, junto con procesos y protocolos de trabajo conjunto claramente definidos. En 2008, el CdE publicó Directrices para la cooperación entre las autoridades de aplicación de la ley y los PSI en la lucha contra la ciberdelincuencia.[104]

Medidas técnicas

Son muchas las medidas técnicas basadas en procesos – que deberían conjugarse con otras medidas – que pueden ayudar en la lucha contra el abuso sexual infantil. A menudo, se combinan los mecanismos de información de atención telefónica directa y las solicitudes de detección y eliminación. La Asociación Internacional de Líneas Directas de Denuncia de Internet (INHOPE), una red de colaboración de 51 líneas de 45 países (hasta la fecha), procesa miles de informes anualmente, la mayoría de los cuales llega a las agencias de aplicación de la ley dentro de las 24 horas siguientes a la denuncia. Otras medidas técnicas incluyen mantener una base de datos de identificación de víctimas y evitar el acceso a ciertos sitios, junto con el registro de huellas digitales, la minería de datos, y análisis para colaborar en las investigaciones.

Creación de conciencia y educación

A nivel nacional, regional, e internacional, tuvieron lugar muchas campañas dirigidas a niños y jóvenes, padres y tutores, y educadores. También hay una gran cantidad de recursos de concientización disponibles en línea. La Protección de la Infancia en Línea (COP, por sus siglas en inglés) de la UIT brinda directrices para niños, padres y tutores, educadores, la industria, y los legisladores.[105] La Red de Centros para una Internet más Segura (INSAFE en inglés), una red europea de 31 centros de concientización nacionales, proporciona un conjunto de herramientas para las familias en diferentes idiomas. El Día de Internet Segura, celebrado en varios países en febrero, está destinado a promover un uso más seguro de Internet, especialmente entre niños y jóvenes en todo el mundo.

Enfoque coordinado

La protección infantil en línea, y la lucha contra el abuso y la explotación sexual infantil también exigen un esfuerzo concertado de las partes interesadas, quienes deben actuar juntas en una manera efectiva y coordinada.

Los padres y educadores tienen la responsabilidad de guiar y respaldar a los niños, y desempeñan un rol importante en la educación y la concientización, consideradas la primera línea de defensa importante. Los gobiernos tienen la responsabilidad primordial de proteger a los niños, y en muchos países, la protección infantil en línea se encuentra como uno de los primeros temas en las agendas políticas nacionales. La aplicación de la ley cumple un rol importante en lograr que la Internet sea segura y esté libre de criminales, y también trabaja a nivel regional e internacional para combatir el abuso sexual infantil en línea. La Oficina Europea de Policía (Europol, en inglés) y la Organización Internacional de Policía

Criminal (INTERPOL) operan varias bases de datos para ayudar a identificar víctimas de abuso sexual infantil.

La industria tiene la responsabilidad de asegurar que el entorno en línea sea seguro y esté protegido. Los proveedores de servicios pueden desempeñar un papel importante en la creación de ese entorno, y se puede recurrir a muchas herramientas – como los filtros y los mecanismos de denuncia – para lograrlo. Las coaliciones de industrias incluyen a la Coalición de Tecnologías; las coaliciones financieras cuentan con la Coalición Financiera contra la Pornografía Infantil de EE. UU., la Coalición Financiera Asia-Pacífico, y la Coalición Financiera Europea; y la Alianza Móvil contra contenidos de abuso sexual infantil de la GMSA.

Muchos profesionales expertos en el tema probablemente estén activos en organizaciones de la sociedad civil, lo que puede proporcionar una contribución invaluable mediante el conocimiento y la experiencia. Las ONG nacionales pueden cooperar por medio de redes internacionales, como la ECPAT International y el ICMEC. Varias iniciativas y organizaciones regionales también se concentran en la seguridad infantil en línea.

Las ONG para los niños y las líneas de asistencia infantil también son partes clave en la lucha contra el abuso y la explotación sexual infantil – tanto en línea como fuera de línea – y son compañeros valiosos en el entendimiento de la magnitud y naturaleza del problema, así como también en la facilitación de consejos y apoyo para las víctimas de abusos.

www.igbook.info/childsafety

NOTAS FINALES

1 Radunović V (2013) DDoS – Available Weapon of Mass Disruption. *Proceedings of the 21st Telecommunications Forum (TELFOR)*, 26–28 de noviembre, Belgrado, Serbia, pp. 5–9.

2 Goodin D (2015) Botnet that enslaved 770,000 PCs worldwide comes crashing down. *Arstechnica*, 13 de abril. Disponible en http://arstechnica.com/security/2015/04/botnet-that-enslaved-770000-pcs-worldwide-comes-crashing-down/ [accedido el 21 de octubre de 2016].

3 ONU (1999) Resolución de la Asamblea General: Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional. A/RES/53/70. Disponible en http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70 [accedido el 8 de febrero de 2016].

4 Naciones Unidas (2015) Informe del Grupo de Expertos Gubernamentales sobre el avance en la informatización y las telecomunicaciones en el contexto de la seguridad internacional *Informe*. Disponible en http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [accedido el 6 de junio de 2016].

5 Grigsby A (2015) The UN GGE on cybersecurity: What is the UN's role? *Council on Foreign Relations Blog*, 15 de abril. Disponible en http://blogs.cfr.org/cyber/2015/04/15/the-un-gge-on-cybersecurity-what-is-the-uns-role/ [accedido el 8 de febrero de 2016].

6 UTI (sin fecha) Agenda sobre Ciberseguridad Global. Disponible en http://www.itu.int/osg/csd/cybersecurity/gca/ [accedido el 22 de octubre de 2016].

7 UIT (sin fecha) Índice Mundial de Ciberseguridad. Disponible en http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx [accedido el 22 de octubre de 2016].

8 DiploFoundation (2015) Resumen del IGF. Just-in-time Reporting from the 2015 Internet Governance Forum. Disponible en http://digitalwatch.giplatform.org/sites/default/files/IGFReportWEB.pdf [accedido el 8 de febrero de 2016].

9 Hague W (2011) London Conference on Cyberspace – Chairman's Summary. Disponible en https://www.gccs2015.com/sites/default/files/documents/London%20Conference%20on%20Cyberspace%20-%20Chair's%20Summary%20-%201-2%20Nov%202011%20_1_.pdf [accedido el 8 de febrero de 2016].

10 Foro Global de Experticia Cibernética (2015) Declaración de La Haya sobre el GFCE. Disponible en http://www.thegfce.com/documents/publications/2015/04/16/the-hague-declaration-on-the-gfce [accedido el 22 de octubre de 2016].

11 Declaración del Secretario General de la OTAN tras la reunión del Consejo del Atlántico Norte en el marco de los Ministros de Defensa de la OTAN, disponible en http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en [accedido el 12 de agosto de 2016].

12 Centro de Excelencia OTAN de Ciberdefensa Cooperativa (2013) Manual de Tallín sobre la Ley Internacional aplicable a la Ciberguerra. Disponible en https://ccdcoe.org/research.html [accedido el 22 de octubre de 2016].

13 Klimburg A (Ed.) (2012) Manual sobre el Marco Nacional de Ciberseguridad. Publicación del Centro de Excelencia OTAN de Ciberdefensa Cooperativa. Disponible en https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf [accedido el 22 de octubre de 2016].

14 Consejo de Europa (2001) Convenio sobre Ciberdelincuencia. Disponible en http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [accedido el 21 de octubre de 2016].

15 Unión Europea (2013) Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro. Disponible en https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-–-open-safe-and-secure-cyberspace [accedido el 22 de octubre de 2016].

16 Unión Europea (2016) Directiva (UE) 2016/1148 del Parlamento Europeo y el Consejo del 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad

de las redes y sistemas de Información en la Unión. Disponible en http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG [accedido el 18 de agosto de 2016].

17 OSCE (2013) Decisión No. 1106 Conjunto Inicial de Medidas de la OSCE para el fomento de la Confianza destinadas a Reducir los Riesgos de Conflicto dimanantes del Uso de Tecnologías de la Información y la Comunicación. Disponible en http://www.osce.org/pc/109168?download=-true [accedido el 22 de octubre de 2016].

18 OSCE (2016) Decisión No. 1202 Medidas de la OSCE para el Fomento de la Confianza destinadas a Reducir los Riesgos de Conflicto dimanantes del Uso de Tecnologías de la Información y la Comunicación. Disponible en http://www.osce.org/pc/227281?download=true [accedido el 22 de octubre de 2016].

19 Organización de los Estados Interamericanos (2003) AG/RES. 1939 (XXXIII-O/03. Resolución de la Asamblea General: Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética. Disponible en http://www.oas.org/juridico/english/agres_1939.pdf [accedido el 22 de octubre de 2016].

20 Organización de los Estados Americanos (2011) Portal Interamericano en Delito Cibernético. Disponible en http://www.oas.org/juridico/english/cyber.htm [accedido el 8 de febrero de 2016].

21 Foro Regional ASEAN (2012) Declaración de los Ministros de Relaciones Exteriores sobre la Cooperación para Asegurar la Ciberseguridad. Disponible en https://ccdcoe.org/sites/default/files/documents/ASEAN-120712-ARFStatementCS.pdf [accedido el 8 de febrero de 2016].

22 ASEAN (2014) Medidas de Construcción de Confianza de ASEAN. Presentación de la Secretaría de ASEAN. UNIDIR. Estabilidad Cibernética: Seminario «Preventing Cyber Conflict», 10 de febrero de 2014, Ginebra, Suiza. Disponible en http://www.unidir.ch/files/conferences/pdfs/the-asean-s-cyber-confidence-building-measures-en-1-958.pdf [accedido el 8 de febrero de 2016].

23 Grigsby A (2015) Will China and Russia's updated code of conduct get more traction in a post-Snowden era? *Council on Foreign Relations Blog*, 28 de enero. Disponible en http://blogs.cfr.org/cyber/2015/01/28/will-china-and-russias-updated-code-of-conduct-get-more-traction-in-a-post-snowden-era/ [accedido el 22 de octubre de 2016].

24 Unión Africana (2014) Convenio de la Unión Africana sobre la Ciberseguridad y la Protección de Datos Personales. Disponible en http://www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection accedido el 6 de junio de 2016].

25 Microsoft (2015) Normas internacionales en materia de ciberseguridad: Reducción de conflictos en un mundo que depende de Internet. Disponible en http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-56836FD44/International_Cybersecurity_%20Norms.pdf [accedido el 8 de febrero de 2016].

26 Para obtener un análisis pormenorizado sobre la interacción de este triángulo de políticas, lea el informe del Taller del IGF 2015: Cybersecurity, human rights and Internet business triangle. Disponible en http://digitalwatch.giplatform.org/sessions/cybersecurity-human-rights-and-Internet-business-triangle [accedido el 6 de junio de 2016].

27 Explicación de las Extensiones de Seguridad para el Sistema de Nombres de Dominio. Disponible en http://everything.explained.at/DNSSEC/ [accedido el 21 de octubre de 2016].

28 Radunović V (2013) Waging a (private) cyber war. Disponible en http://www.diplomacy.edu/blog/waging-private-cyberwar [accedido el 22 de octubre de 2016].

29 Perlroth N and Gellese D (2014) Russian gang said to amass more than a billion stolen Internet credentials. *New York Times,* 5 de agosto. Disponible en http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-Internet-credentials.html?_r=0 [accedido el 22 de octubre de 2016].

30 *RT* (2014) Brazil and the EU have pushed forward their dialogue on developing a direct submarine link. 24 de febrero. Disponible en http://rt.com/news/brazil-eu-cable-spying-504/ [accedido 22 de octubre de 2016].

31 Keck Z (2014) China expands cyber spying. *The Diplomat*, 12 de abril. Disponible en http://thediplomat.com/2014/04/china-expands-cyber-spying/ [accedido el 22 de octubre de 2016].

[32] Ranger S (2014) We're the real hacking victims, says China. *ZDNet*, 20 de mayo. Disponible en http://www.zdnet.com/were-the-real-hacking-victims-says-china-7000029666/ [accedido el 22 de octubre de 2016].

[33] Spetalnick M and Martina M (2015) Obama announces 'understanding' with China's Xi on cyber theft but remains wary. *Reuters*, 26 de septiembre. Disponible en http://www.reuters.com/article/us-usa-china-idUSKCN0RO2HQ20150926 [accedido el 8 de febrero de 2016].

[34] G20 (2015) Comunicado de Líderes del G20. Cumbre de Antalya, 15-16 de noviembre de 2015. Disponible en http://g20.org/English/Documents/PastPresidency/201512/P020151228335504307519.pdf [accedido el 8 de febrero de 2016].

[35] Schneier B (2013) NSA surveillance: A guide to staying secure. *The Guardian*, 6 de septiembre. Disponible en www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance [accedido el 22 de octubre de 2016].

[36] Para ver una lista de redes, organizaciones, e iniciativas mundiales contra la ciberdelincuencia, diríjase a la página de recursos del CdE. Disponible en http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/networks/Networks_en.asp [accedido el 22 de octubre de 2016].

[37] El Commonwealth (sin fecha) Iniciativa contra la Ciberdelincuencia del Commonwealth. Disponible en http://thecommonwealth.org/commonwealth-cybercrime-initiative [accedido el 22 de octubre de 2016].

[38] Bailey C (2002) The International Convention on Cybercrime. Asociación para el Progreso de las Comunicaciones. Disponible en http://rights.apc.org/privacy/treaties_icc_bailey.shtml [accedido el 7 de marzo de 2016].

[39] Consejo de Europa (2014) Recomendación CM/Rec(2014)6 del Comité de Ministros para los estados miembros en la Guía de los derechos humanos para los usuarios de Internet. Disponible en https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31 [accedido el 20 de octubre de 2016].

[40] Unión Europea (2006) Directiva 2006/24/CE del Parlamento Europeo y el Consejo del 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF [accedido el 22 de octubre de 2016].

[41] Para obtener una revisión detallada de los problemas de la conservación de datos en la UE, consulte a la Comisión Europea (2011) Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE). Disponible en http://www.publications.parliament.uk/pa/cm201012/cmselect/cmeuleg/428-xxix/42816.htm [accedido el 22 de octubre de 2016].

[42] TJUE (2014) Sentencia en los asuntos acumulados C-293/12 y C-594/12: Digital Rights Ireland vs Minister for Communications, Marine and Natural Resources y otros. Disponible en http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=106306 [accedido el 22 de octubre de 2016].

[43] Comisión Europea (2004) Protección de Infraestructuras Críticas en la lucha contra el terrorismo. Comunicación de la Comisión al Consejo y al Parlamento Europeo. Disponible en http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0702&from=EN [accedido el 22 de octubre de 2016].

[44] Essers L (2014) Cyberattack on German steel factory causes 'massive damage'. *IT World*, 19 de diciembre. Disponible en http://www.itworld.com/article/2861675/cyberattack-on-german-steel-factory-causes-massive-damage.html [accedido el 22 de octubre de 2016].

[45] IETF (2007) Internet Security Glossary, Version 2. Disponible en https://tools.ietf.org/html/rfc4949 [accedido el 18 de agosto de 2016].

[46] Casa Blanca EE. UU. (2013) Presidential Policy Directive – Critical Infrastructure Security and Resilience. Disponible en https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [accedido el 18 de agosto de 2016].

[47] Comisión Europea (2006) Programa Europeo de Protección de Infraestructuras Vitales. Disponible en http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l33260 [accedido el 18 de agosto de 2016].

[48] Unión Europea (2008) Consejo. Directiva 2008/114/CE del 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. Disponible en http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008L0114 [accedido el 18 de agosto de 2016].

[49] OECD (2008) Recomendación del Consejo sobre protección de infraestructuras críticas de información. Disponible en http://webnet.oecd.org/OECDACTS/Instruments/ShowInstrumentView.aspx?InstrumentID=121&InstrumentPID=117&Lang=en&Book= [accedido el 22 de octubre de 2016].

[50] The Cyberterrorism Project (2013) What is cyberterrorism? Definición Jurídica. Reino Unido. Disponible en http://www.cyberterrorism-project.org/what-is-cyberterrorism/ [accedido el 22 de octubre de 2016].

[51] Krasavin S (2009) What is Cyber-terrorism? Computer Crime Research Center. Disponible en http://www.crime-research.org/library/Cyber-terrorism.htm [accedido el 22 de octubre de 2016].

[52] Denning D (2000) Statement. Disponible en http://fas.org/irp/congress/2000_hr/00-05-23denning.htm [accedido el 22 de octubre de 2016].

[53] Comunicado conjunto sobre el balance de la reunión de los Ministros de Asuntos Exteriores de Rusia, la República de la India y la República Popular China, 18 de abril de 2016. Disponible en http://mea.gov.in/bilateral-documents.htm?dtl/26628/Joint_Communiqu_of_the_14th_Meeting_of_the_Foreign_Ministers_of_the_Russian_Federation_the_Republic_of_India_and_the_Peoples_Republic_of_China [accedido el 22 de octubre de 2016].

[54] *Centro de Noticias de la ONU* (2016) Security Council requests UN panel to propose global framework on countering terrorist propaganda. 11 de mayo. Disponible en http://www.un.org/apps/news/story.asp?NewsID=53909#.WAszjTeZIqZ [accedido el 22 de octubre de 2016].

[55] G7 (2016) Plan de acción del G7 para combatir el terrorismo y el extremismo violento. Disponible en http://www.mofa.go.jp/files/000160278.pdf [accedido el 22 de octubre de 2016].

[56] Microsoft (2016) Microsoft's approach to terrorist content online. Disponible en http://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/#sm.000kpo9tsyeqeho11lj2rn85kklld [accedido el 22 de octubre de 2016].

[57] Greenberg A (2016) Google's clever plan to stop aspiring ISIS recruits. *Wired*, 17 de septiembre. Disponible en https://www.wired.com/2016/09/googles-clever-plan-stop-aspiring-isis-recruits/ [accedido el 22 de octubre de 2016].

[58] *Centro de Noticias de la ONU* (2016) UN expert warns combat against violent extremism could be used as 'excuse' to curb free speech. 3 de mayo. Disponible en http://www.un.org/apps/news/story.asp?NewsID=53841#. WAs1FjeZIqb [accedido el 22 de octubre de 2016].

[59] *GCN* (2012) DOD wants cyberterrorism-prediction software. 31 de julio. Disponible en http://gcn.com/articles/2012/07/31/agg-dod-small-biz-software-support.aspx [accedido el 22 de octubre de 2016].

[60] Proyecto Clean IT (2012). Disponible en http://www.cleanitproject.eu/about-the-project/ [accedido el 18 de agosto de 2016].

[61] Asamblea General de las Naciones Unidas (2006) Resolución A/60/288. Estrategia Global de las Naciones Unidas contra el Terrorismo. Disponible en http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/60/288 [accedido el 22 de octubre de 2016].

[62] UNODC (2012) El uso de Internet con fines terroristas. Disponible en: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [accedido el 22 de octubre de 2016].

[63] Consejo de Seguridad de la ONU – Comité contra el Terrorismo (2015) Special Meeting of the Counter-Terrorism Committee and technical sessions of the Counter-Terrorism Committee Executive Directorate on preventing and combating abuse of ICT for terrorist purposes. Disponible en http://www.un.org/en/sc/ctc/news/2015-11-18_CTED_SpecialMeeting_ICT.html [accedido el 22 de octubre de 2016].

[64] Berenger RD (2012) Cyber Warfare. In Yan Z [ed] Encyclopedia of Cyber Behavior. Hershey, PA: Information Science Reference, pp. 1074–1087.

[65] *BBC News* (2007) Estonia hit by 'Moscow cyber war'. 17 de mayo. Disponible en http://news.bbc.co.uk/2/hi/europe/6665145.stm [accedido el 22 de octubre de 2016].

[66] Swaine J (2008) Georgia: Russia 'conducting cyber war'. *The Telegraph*, 11 de agosto. Disponible en http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html [accedido el 22 de octubre 2016].

[67] Sanger D (2012) Obama sped up wave of cyberattacks against Iran. *New York Times*, 1 de junio. Disponible en http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [accedido el 22 de octubre de 2016].

[68] Nakashima E (2012) Iran blamed for cyberattacks on U.S. banks and companies. *The Washington Post*, 21 de septiembre. Disponible en http://articles.washingtonpost.com/2012-09-21/world/35497878_1_web-sites-quds-force-cyberattacks [accedido el 22 de octubre de 2016].

[69] Lee C and Solomon J (2015) US targets North Korea in retaliation for Sony hack. *The Wall Street Journal*, 3 de enero. Disponible en http://www.wsj.com/articles/u-s-penalizes-north-korea-in-retaliation-for-sony-hack-1420225942 [accedido el 22 de octubre de 2016].

[70] Foster P (2013) China denies Pentagon cyber-attack claims. *The Telegraph*, 7 de mayo. Disponible en http://www.telegraph.co.uk/news/worldnews/asia/china/10040757/China-denies-Pentagon-cyber-attack-claims.html [accedido el 22 de octubre de 2016].

[71] Ranger S (2014) We're the real hacking victims, says China. *ZDNet*, 20 de mayo. Disponible en http://www.zdnet.com/were-the-real-hacking-victims-says-china-7000029666/ [accedido el 22 de octubre de 2016].

[72] Conferencia de seguridad de Múnich (2015) Collapsing Order, Reluctant Guardians? Informe de Seguridad de Múnich 2015. Conferencia de Seguridad de Múnich. Disponible en https://www.securityconference.de/en/activities/munich-security-report/ [accedido el 22 de octubre de 2016].

[73] Radunović V (2013) DDoS – Available Weapon of Mass Disruption. *Proceedings of the 21st Telecommunications Forum (TELFOR)*, 26–28 de noviembre, Belgrado, Serbia, pp. 5–9.

[74] Appelbaum *et al.* (2014) Prying Eyes: Inside the NSA's War on Internet Security. *Der Spiegel,* 28 de diciembre. Disponible en http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-Internet-security-a-1010361.html [accedido el 11 de agosto de 2016].

[75] El Acuerdo de Wassenaar. Disponible en http://www.wassenaar.org/ [accedido el 22 de octubre de 2016].

[76] El gobierno de EE. UU. propuso el enfoque Clipper en 1993. Tenía como eje central el uso de un chip Clipper que supuestamente usarían todos los teléfonos y otras herramientas de comunicación por voz. El chip Clipper tenía una «puerta trasera» que podrían haber utilizado los gobiernos para la vigilancia lícita. Tras una fuerte oposición por parte de los activistas de derechos humanos y el público en general, el gobierno de EE. UU. retiró la propuesta en 1995. Denning D (1995) The case for clipper. *MIT Technology Review.* MIT: Cambridge, MA, EE. UU. Disponible en http://encryption_policies.tripod.com/us/denning_0795_clipper.htm [accedido el 22 de octubre de 2016].

[77] Huggler J (2015) Man arrested in Germany on suspicion of illegal arm dealing in terror crackdown. *The Telegraph,* 27 de noviembre. Disponible en http://www.telegraph.co.uk/news/worldnews/europe/germany/12020249/Paris-attackers-bought-weapons-from-arms-dealer-in-Germany.html [accedido el 11 de agosto de 2016].

[78] Un estudio publicado por el Centro Berkman para Internet y la Sociedad en la Universidad de Harvard afirma que «la metáfora "going dark" [la terminación de la comunicación] no describe completamente el futuro de la capacidad del gobierno de acceder a las comunicaciones de los sospechosos de terrorismo y criminales. La creciente disponibilidad de las tecnologías de cifrado impide la vigilancia gubernamental bajo ciertas circunstancias, y en este sentido, el gobierno está perdiendo algunas oportunidades de vigilancia. Sin embargo, [...] la combinación de desarrollos tecnológicos y fuerzas del mercado probablemente llene algunos de estos vacíos y, en términos más generales, asegure que el gobierno obtendrá nuevas oportunidades para recopilar información crucial mediante la vigilancia». Para obtener más detalles, vea: Centro Berkman para Internet y la Sociedad de la Universidad de Harvard (2016). Don't Panic. Making Progress on the 'Going Dark' Debate. Disponible en https://cyber.law.harvard.edu/pubrelease/

dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [accedido el 12 de julio de 2016].

79 Un estudio que investigó a 865 productos de *hardware* y *software* con cifrado incorporado, en 55 países, señala que, debido a la amplia disponibilidad de estos productos, cualquier puerta trasera obligatoria exigida por las autoridades de aplicación de la ley «será inefectiva». Esto sucede gracias a que dichas puertas traseras son fáciles de evitar, dado que el mercado para los productos de cifrado es internacional, y los delincuentes pueden cambiarse a productos que no están cubiertos por la legislación nacional en una determinada jurisdicción. En cambio, cualquier puerta trasera obligatoria por ley nacional afectara a los «usuarios inocentes de dichos productos», dejando a las personas del país del que se trate «vulnerables al abuso de esas puertas traseras por parte de ciberdelincuentes y otros gobiernos». Para obtener más detalles, consulte Schneier B, Seidel K y, Vijayakumar S (2016) A Worldwide Survey of Encryption Products. Disponible en https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf [accedido el 12 de julio de 2016].

80 El informe está disponible en http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32 [accedido el 12 de julio de 2016].

81 DiploFoundation (2016) Apple vs FBI: A Socratic dialogue on privacy and security. Disponible en http://www.diplomacy.edu/blog/apple-vs-fbi-socratic-dialogue-privacy-and-security [accedido el 11 de agosto de 2016].

82 El troyano financiero Dridex provocó graves preocupaciones en 2016. Las compañías de ciberseguridad lo describieron como «una de las amenazas en línea más graves que enfrentan los consumidores y las empresas». El troyano, distribuido mediante grandes campañas de correo no deseado, es capaz de recopilar credenciales bancarias de cientos de clientes de bancos y otras instituciones financieras alrededor del mundo. Para obtener más detalles, lea: O'Brien D (2016) Dridex: Tidal waves of spam pushing dangerous financial Trojan. Symantec. Disponible en http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf [accedido el 14 de julio de 2016].

83 Reporte de Seguridad Global de Trustwave (2016). Disponible en https://www2.trustwave.com/rs/815-RFM-693/images/2016%20Trustwave%20Global%20Security%20Report.pdf [accedido el 13 de julio de 2016].

84 Gudkova D, Vergelis M, Demidova N y Shcherbakova T (2016) Informe de Spam y Phishing de Q1 de 2016. Kaspersky Lab. Disponible en https://securelist.com/analysis/quarterly-spam-reports/74682/spam-and-phishing-in-q1-2016/ [accedido el 13 de julio de 2016].

85 La manera en que funciona Locky es simple: engaña a los usuarios a abrir adjuntos maliciosos enviados mediante correos electrónicos no deseados. Una vez instalado en los dispositivos de los usuarios, el troyano cifra todos los datos y se le pide al usuario que pague el rescate para descifrar sus archivos. Para obtener más información sobre Locky, lea: Sinitsyn F (2016) Locky: the encryptor taking the world by storm. Kaspersky Lab. Disponible en https://securelist.com/blog/research/74398/locky-the-encryptor-taking-the-world-by-storm/ [accedido el 14 de julio de 2016].

86 Más referencias sobre la ley Can-Spam se encuentran disponibles en el Buró de Protección al Consumidor (2009). The CAN-SPAM Act: A Compliance Guide for Business. Disponible en https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business[accedido el 22 de octubre de 2016].

87 En junio de 2016, un ciudadano estadounidense fue sentenciado a dos años y medio de privación de la libertad y se le ordenó pagar la suma de USD 310.628,55 en compensación por haber enviado 27 millones de mensajes no deseados a usuarios de Facebook. Según la Fiscalía General del Distrito Norte de California, el hombre, de manera ilícita, obtuvo, almacenó, y explotó la información de los usuarios de Facebook y ganó dinero dirigiendo a los usuarios a otros sitios web. El esquema, ejecutado entre noviembre de 2008 y marzo de 2009, comprometió aproximadamente a 500.000 cuentas de Facebook legítimas. Para obtener más detalles, lea el comunicado de prensa de la Fiscalía General del Distrito Norte de California. Disponible en https://www.justice.gov/usao-ndca/pr/sanford-spam-king-wallace-sentenced-two-and-half-years-custody-spamming-facebook-users [accedido el 13 de julio de 2016].

[88] Unión Europea (2012) Directiva 2002/58/CE del Parlamento Europeo y del Consejo del 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Disponible en http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002L0058 [accedido el 22 de octubre de 2016].

[89] *BBC NEWS* (2004) European anti-spam laws lack bite. 28 de abril. Disponible en http://news.bbc.co.uk/2/hi/technology/3666585.stm [Accedido el 13 de febrero de 2014].

[90] New Zealand Law Society (2016) NZ signatory to international anti-spam MOU. 15 de junio. Disponible en https://www.lawsociety.org.nz/news-and-communications/latest-news/news/nz-signatory-to-international-anti-spam-mou [accedido el 22 de octubre de 2016].

[91] UIT (2012) Resolución 52 Asamblea Mundial de Normalización de las Telecomunicaciones: Respuesta y lucha contra el correo basura. Disponible en https://www.itu.int/en/ITU-T/wtsa12/Documents/resolutions/Resolution%2052.pdf [accedido el 22 de octubre de 2016].

[92] APEC (2012) Principios para la Acción contra el Spam de APEC. Disponible en http://www.apec.org/Meeting-Papers/Sectoral-Ministerial-Meetings/Telecommunications-and-Information/2005_tel/annex_e.aspx [accedido el 22 de octubre de 2016].

[93] Unión Africana (2014) Convenio de la Unión Africana sobre la Ciberseguridad y la Protección de Datos Personales. Disponible en http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf [accedido el 22 de octubre de 2016].

[94] Para ver estadísticas actualizadas sobre los países que permiten el correo no deseado, lea sobre el Proyecto Spamhaus, disponible en https://www.spamhaus.org/statistics/countries/ [accedido el 14 de julio de 2016]. El Proyecto también brinda información estadística sobre los varios problemas relacionados con el correo no deseado, como los PSI que apoyan el correo no deseado, los peores *spammers*, los países con el más alto número de robots de correo no deseado, los TLD más propensos al abuso por parte del correo no deseado, etc.

[95] La autenticación y verificación de un registro electrónico mediante el uso de algoritmos criptográficos; el término «firma electrónica» es más amplio e incluye una amplia variedad de técnicas de autenticación, como la firma digital y la biometría.

[96] Para obtener una explicación más detallada de estos tres enfoques, consulte: ILPF (1999) Survey of International Electronic and Digital Signature Initiatives. Disponible en http://www.ilpf.org/groups/survey.htm#IB [accedido el 21 de agosto de 2016].

[97] Unión Europea (2014) Reglamento (UE) No. 910/2014 sobre la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Disponible en http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG [accedido el 12 de agosto de 2016].

[98] UNCITRAL (2001) Ley Modelo sobre las Firmas Electrónicas. Disponible en http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2001Model_signatures.html [accedido el 22 de octubre de 2016].

[99] Longmuir G (2000) Privacy and Digital Authentication. Disponible en www.longmuir.net/papers/Research%20Paper.doc [accedido el 20 de agosto de 2016]. Este documento se centra en los aspectos personales, comunitarios, y gubernamentales de la necesidad de contar con la autenticación en un mundo digital.

[100] 1De acuerdo con los instrumentos y prácticas internacionales, un «niño» es una persona que tiene menos de 18 años.

[101] 1Typologies include: Barbosa A *et al.* (2013) Risks and Safety on the Internet: Comparing Brazilian and European Results. London: LSE. Disponible en http://www.lse.ac.uk/media@lse/research/Research-Projects/Researching-Childrens-Rights/pdf/Barbosa-et-al-%282013%29.-Risks-and-safety-on-the-Internet.-Comparing-Brazilian-and-European-children.pdf [accedido el 9 de agosto de 2016]; OCDE (2012) Recomendación del Consejo de la OCDE sobre la Protección de los Niños en Línea. Disponible en http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf [accedido el 9 de agosto de 2016].

[102] EU Kids Online (2014) EU Kids Online: Findings, Methods, Recommendations. London: LSE. Disponible en http://eprints.lse.ac.uk/60512/ [accedido el 9 de agosto de 2016].

[103] 1El término «pornografía infantil» plantea un problema, ya que se lo asocia típicamente a las representaciones de actividad sexual entre adultos mayores de edad. Debido a que el término no consigue destacar los aspectos abusivos y de explotación, se lo evita cada vez más para favorecer a nuevos términos, como «contenido de abuso sexual infantil», y «contenido de explotación sexual infantil». Interagency Working Group on Sexual Exploitation of Children (2016) Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Disponible en http://www.ilo.org/wcmsp5/groups/public/---ed_norm/---ipec/documents/instructionalmaterial/wcms_490167.pdf [accedido el 12 de agosto de 2016].

[104] Consejo de Europa (2008) Directrices para la cooperación entre las autoridades responsables de velar por el cumplimiento de la ley y los proveedores de servicios de Internet en la lucha contra la ciberdelincuencia. Disponible en https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3ba [accedido el 22 de octubre de 2016].

[105] 1UIT (sin fecha) Directrices para la Protección de la Infancia en Línea. Disponible en http://www.itu.int/en/cop/Pages/guidelines.aspx [accedido el 22 de octubre de 2016].

Sección 4

LA CANASTA LEGAL

La canasta legal

Las funciones sociales básicas de la ley siguen siendo tan relevantes en Internet como lo eran hace miles de años, cuando nuestros antepasados empezaron a usar reglas para organizar la sociedad humana. La ley regula los derechos y responsabilidades entre los individuos y las entidades que estos establecen, desde compañías hasta estados nacionales. El orden público y la certeza jurídica son esenciales para el mayor crecimiento de Internet, como medio de comunicación social, y como vehículo para el desarrollo económico.

La regulación jurídica de Internet ha evolucionado desde el ciberderecho hasta el enfoque del derecho real. En los primeros días de Internet, el enfoque del ciberderecho prevalecía, en base de la presunción de que la Internet introdujo nuevas formas de relaciones sociales en el ciberespacio. Consecuentemente, existía la necesidad de formular nuevas ciberleyes para regular el ciberespacio. Un argumento a favor de este enfoque era que la mera velocidad y el volumen de la comunicación transfronteriza facilitada por la Internet obstaculizarían la aplicación de las normas jurídicas existentes. Otro argumento frecuente era que la regulación tradicional (por ejemplo, relacionada con el crimen, o el aspecto impositivo) no sería lo suficientemente efectiva.[1] Sin embargo, es importante tener en cuenta que las leyes no hacen imposible la conducta prohibida, sólo la hacen punible.

Más recientemente, sin embargo, con la inclusión de Internet en la vida social, el enfoque del derecho real ha cobrado más prominencia. Según este enfoque, se trata a la Internet de una manera que, en su esencia, no es diferente de las tecnologías de telecomunicación previas, en el largo camino de la evolución desde las señales de humo hasta el teléfono. Consecuentemente, las normas jurídicas existentes pueden aplicarse también a Internet. Por ejemplo, el informe de 2013 del GGE de la ONU reiteró que el derecho internacional existente aplica al uso de las TIC por parte del estado.[2] Luego, la Asamblea General de la ONU recibió con brazos abiertos esta conclusión, durante el proceso de revisión de la CMSI+10.[3] En el campo de los derechos humanos, las resoluciones de la Asamblea General de la ONU y el Consejo de Derechos Humanos (CDH) establecieron firmemente el principio por el que los mismos derechos humanos que las personas gozan fuera de línea también deben aplicar en línea.[4]

Aunque existe una respuesta positiva al interrogante sobre si el derecho existente es aplicable a la Internet, la pregunta que queda sin responder es *cómo* implementar esas normas. Por ejemplo, un reto importante es asegurar la reparación jurídica en casos relacionados con la Internet que contengan elementos internacionales. Las personas y las compañías pueden confiar en el derecho privado internacional, mientras que los gobiernos nacionales pueden utilizar mecanismos del derecho público internacionales. Ambos enfoques tienen una larga tradición, y originalmente se desarrollaron en una era de intercambios menos intensos a escala trasfronteriza. Se debe llevar a cabo una investigación acerca de estos enfoques y, en caso de ser necesario, se debe introducir nuevos desarrollos en ellos para proporcionar un acceso asequible a la justicia en cuestiones de Internet para los individuos y las instituciones de todo el mundo.

Instrumentos legales

Una amplia variedad de instrumentos jurídicos ya han sido aplicados o podrían ser aplicados al campo de Internet. Se clasifican como instrumentos aplicables a nivel nacional, e instrumentos aplicables a nivel internacional.

Instrumentos jurídicos nacionales, normas sociales, y autorregulación

La mayor parte de la regulación jurídica de Internet tiene lugar a nivel nacional. Esto crea una tensión inevitable con la comunicación de Internet, que por naturaleza es predominantemente transfronteriza. Algunas resoluciones judiciales, como el caso del derecho al olvido, tienen un mayor impacto más allá de su territorio jurisdiccional. Se espera que los ciudadanos y compañías usen cada vez más los tribunales nacionales (en el caso de la UE, el TJUE) para proteger sus derechos legales e intereses en Internet.

Legislación

Las actividades legislativas se intensificaron de manera progresiva en el campo de Internet. Este es el caso, especialmente, de los países en donde el uso de la Internet está generalizado y tiene un alto impacto en las relaciones económicas y sociales. Hasta el día de hoy, las áreas de prioridad para la legislación de Internet han sido la privacidad y la protección de datos, la propiedad intelectual, la tributación, y la ciberdelincuencia.

El continuo progreso en el campo tecnológico también resultó en la adopción del principio de neutralidad tecnológica, que debe seguirse en la elaboración de la legislación que aborda temas relacionados con la tecnología. En la práctica, este principio quiere decir que la ley no debería hacer una referencia explícita a tecnologías específicas, o favorecer a una tecnología y no a otra; en cambio, se deben utilizar términos generales que permitan que la ley permanezca neutral.

Aun así, las relaciones sociales son demasiado complicadas como para ser reguladas solamente por los legisladores. La sociedad es dinámica y la legislación siempre queda rezagada detrás del cambio social. Esto es particularmente notable hoy en día, ya que los avances tecnológicos están remodelando la realidad social a un ritmo mucho más rápido del que los legisladores pueden mantener. A veces, las normas se vuelven obsoletas incluso antes de entrar en vigencia. El riesgo de la obsolescencia jurídica es una consideración importante en la regulación de Internet.

Normas sociales (costumbres)

Al igual que la legislación, las normas sociales proscriben comportamientos determinados. A diferencia de la legislación, no hay un poder estatal que haga cumplir estas normas. Estas normas se cumplen gracias a la comunidad, mediante la presión de los pares. En sus primeros días, el uso de Internet estaba regulado por un conjunto de normas sociales llamadas «netiquette» (etiqueta en la red), cuyas principales sanciones eran la presión de los pares y la exclusión. Durante este periodo – en el que la Internet era usada principalmente por una comunidad relativamente pequeña, principalmente de académicos – , las normas sociales se cumplían ampliamente. El crecimiento de Internet hizo que estas normas quedaran sin efecto. Este tipo de regulación, sin embargo, aún puede ser utilizada dentro de grupos limitados con fuertes lazos comunitarios. Por ejemplo, la comunidad de Wikipedia está regida por normas sociales que regulan la manera en que se editan los artículos de Wikipedia y la manera en que

se resuelven los conflictos relativos a estos. Mediante la codificación de políticas y guías, las normas de Wikipedia evolucionaron de manera gradual hacia la autorregulación.

Autorregulación

El Libro Blanco sobre Gobernanza de Internet[5] del gobierno de EE. UU. de 1998, que abrió camino a la fundación de ICANN, introdujo la autorregulación como el mecanismo regulatorio preferido para la Internet. La autorregulación cuenta con elementos en común con las normas sociales. La principal diferencia es que, a diferencia de las normas sociales (que típicamente involucran reglas tácitas y difusas) la autorregulación está basada en un conjunto de reglas explícito y bien organizado. Usualmente, la autorregulación codifica un conjunto de reglas de lo que se considera una conducta adecuada o ética.

La tendencia hacia la autorregulación se nota particularmente entre los PSI. En muchos países, los PSI están bajo la creciente presión de las autoridades gubernamentales para hacer cumplir las reglas relacionadas con las políticas de contenido. Los PSI intentan responder a esta presión mediante la autorregulación, al imponer ciertos estándares de comportamiento para sus clientes.

Si bien la autorregulación puede ser una técnica regulatoria útil, quedan algunos riesgos en su uso para la regulación de áreas de alto interés público, como las políticas de contenido, la libertad de expresión, y la protección de la privacidad. Depender de la autorregulación plantea varias preguntas como: ¿Los PSI pueden y deberían tomar decisiones en lugar de las autoridades legales? ¿Pueden y deberían juzgar cuál es el contenido aceptable?

Jurisprudencia

La jurisprudencia (las decisiones judiciales) ha tenido un gran impacto en los desarrollos legales relacionados con Internet. Durante las primeras etapas, cuando la mayor parte del desarrollo ocurría en EE. UU., la jurisprudencia, como piedra angular del sistema legal de EE. UU., cumplió un rol clave en los desarrollos legales relativos a Internet. La Internet, como un nuevo fenómeno, se reguló mediante casos judiciales (precedentes en la ley anglosajona). Los jueces debían resolver casos incluso cuando no tenían las herramientas necesarias; es decir, las reglas jurídicas. Mediante el uso de precedentes, comenzaron a desarrollar una nueva ley.

Más recientemente, la jurisprudencia de los tribunales europeos se ha cobrado una particular importancia para los desarrollos legales en línea. Por ejemplo, la sentencia del TJUE de mayo de 2014 introdujo nuevas reglas sobre el derecho al olvido, o, para ser más específicos, el derecho a desindexación, con consecuencias para el contenido en línea en Europa y otros lugares. Otra sentencia, en octubre de 2015, que declaró inválido el acuerdo Safe Harbour entre EE. UU. y la UE, causó un impacto similar, ya que forzó a las dos partes a negociar y a llegar a un nuevo acuerdo sobre la transferencia de datos personales de un lado al otro del Atlántico.

Consulte la Sección 8 para saber más sobre las sentencias del TJUE en el campo de la protección de la privacidad y los datos personales.

Instrumentos legales internacionales

La naturaleza transfronteriza de las actividades de Internet trae aparejada la necesidad de usar herramientas jurídicas internacionales. En debates sobre el derecho internacional, existe una confusión terminológica que podría provocar consecuencias sustantivas. El término

«derecho internacional» es usado principalmente como sinónimo de «derecho internacional *público*», establecido por estados nacionales, usualmente mediante la adopción de tratados y convenios. El derecho internacional público aplica a muchas áreas de la Internet, como en la de telecomunicaciones, derechos humanos, y ciberdelincuencia, entre tantas otras. Sin embargo, el derecho internacional *privado* es igualmente o incluso más importante para lidiar con los problemas de Internet, debido a que la mayoría de los casos judiciales de Internet contienen aspectos como contratos, ilícitos civiles, y responsabilidades comerciales.

Derecho internacional privado

Dado el carácter global de Internet, son frecuentes las disputas legales que involucran a individuos e instituciones de diferentes jurisdicciones nacionales. Las reglas del derecho internacional privado especifican los criterios para establecer la jurisdicción y la ley aplicables en los casos legales con elementos foráneos (como las relaciones jurídicas que involucran a dos o más entidades de diferentes países), por ejemplo, quién tiene la jurisdicción en posibles casos jurídicos entre compañías de Internet (como Facebook y Twitter) y sus usuarios, esparcidos por todo el mundo. Los criterios de jurisdicción incluyen el vínculo entre un individuo y una jurisdicción nacional (por ejemplo, la nacionalidad, el domicilio) y el vínculo entre una transacción en particular y la jurisdicción nacional (por ejemplo, dónde se celebró el contrato, dónde tuvo lugar el intercambio de bienes).

Sin embargo, rara vez se ha utilizado el derecho internacional privado para resolver problemas basados en Internet, posiblemente porque sus procedimientos son por lo general complejos, lentos, y costosos. Los principales mecanismos del derecho internacional privado se desarrollaron en un momento en el que la interacción transfronteriza era menos frecuente y menos intensa, y, por lo tanto, en proporción había menos casos que involucraban a individuos y entidades de diferentes jurisdicciones. El derecho privado internacional debe ser más rápido, más barato y más flexible a fin de garantizar una reparación legal en los casos legales relacionados con Internet.

Derecho internacional público

El derecho internacional público regula las relaciones entre estados nacionales. Algunos instrumentos del derecho internacional público ya abordan áreas de relevancia para la gobernanza de Internet (por ejemplo, la reglamentación de las telecomunicaciones, los convenios de derechos humanos, los tratados de comercio internacional). Una serie de elementos del derecho internacional público podrían ser usados en la gobernanza de Internet, como los tratados y convenios, el derecho consuetudinario, la legislación «blanda», y el *ius cogens* (derecho vinculante, una norma imperativa).

Convenios internacionales

Los convenios internacionales son acuerdos entre estados legalmente vinculantes. El principal conjunto de convenios que, algunos consideran, abordan temas relacionados con Internet es el RTI de la UIT. Aprobado en 1988, en un momento en que Internet todavía estaba en sus primeras etapas de desarrollo, el RTI no contenía disposiciones específicas sobre Internet. En la WCIT-12 (Conferencia Mundial sobre Telecomunicaciones Internacionales) se mantuvieron debates sobre la posible expansión del RTI para cubrir de manera explícita a la Internet. Se presentaron varias propuestas en ese momento que podrían haber causado un impacto significativo sobre cómo funciona Internet, sobre sus principios subyacentes, así como también sobre la seguridad de Internet y cuestiones relacionadas con su contenido. Los estados miembros no pudieron llegar a un acuerdo en este punto, y el RTI modificado

de 2012 todavía no contiene referencias explícitas a Internet. No obstante, algunos estados miembros de la UIT consideraron que podría interpretarse que varias disposiciones en el RTI modificado cubren cuestiones sensibles relacionadas con Internet, que, en su opinión, deberían estar fuera del alcance de las actividades de la UIT.[6] Estos estados decidieron no firmar el reglamento modificado, por lo que continuaron sujetos a la versión de 1988.

Aparte de los convenios de la UIT, el único que aborda directamente temas relacionados con Internet es el Convenio sobre la Ciberdelincuencia del CdE. Sin embargo, muchos otros documentos jurídicos internacionales son aplicables a cuestiones de Internet: desde la Carta de la ONU hasta instrumentos más específicos que tratan, por ejemplo, los derechos humanos, el comercio, y los IPR.

Derecho internacional consuetudinario

El desarrollo del derecho consuetudinario comprende dos elementos: la práctica general *(consuetudo)* y el reconocimiento del carácter vinculante de tal práctica *(opinio juris)*. Usualmente, el derecho consuetudinario requiere de un lapso prolongado para emerger. Por ejemplo, las normas del derecho marítimo se cristalizaron con el correr de los siglos, mediante prácticas establecidas por los gobiernos nacionales, hasta que estas reglas se codificaron en la Convención sobre el Derecho del Mar de la ONU (1982). Sin embargo, el ritmo acelerado de los avances modernos exige un lapso más corto para el desarrollo de las reglas consuetudinarias. El jurista italiano, Roberto Ago, quien introdujo el concepto de *diritto spontaneo* o «derecho internacional consuetudinario instantáneo» propuso una posible solución para superar la tensión entre el crecimiento acelerado de la Internet y el lento proceso de desarrollo del derecho consuetudinario.[7]

Legislación blanda

El término «legislación blanda» (*soft law*) se usa frecuentemente en los debates sobre la gobernanza de Internet. La mayoría de las definiciones de la legislación blanda se centran en lo que no es: un instrumento legalmente vinculante. Usualmente, los instrumentos de legislación blanda contienen principios y normas que podemos encontrar fácilmente en documentos internacionales como declaraciones y resoluciones. Gracias a que no es legalmente vinculante, la legislación blanda no puede ser aplicada mediante tribunales internacionales u otros mecanismos de resolución de disputas.

Los principales documentos de la CMSI – como la Declaración Final, el Plan de Acción de Ginebra, la Agenda de Túnez para la Sociedad de la Información, y las Declaraciones Regionales – tienen el potencial de desarrollar ciertas normas de legislación blanda. No son legalmente vinculantes, pero por lo general son el resultado de prolongadas negociaciones y aceptación por parte de los estados nacionales. El compromiso que deben asumir los estados nacionales y otras partes interesadas durante las negociaciones de los instrumentos de legislación blanda para llegar a un consenso necesario crea el primer elemento en la consideración de que dichos documentos son más que simples declaraciones políticas.

La legislación blanda trae ciertas ventajas en el abordaje de los asuntos de la gobernanza de Internet. En primer lugar, es un enfoque menos formal, que no requiere ratificación por parte de los estados y, por lo tanto, no precisa de negociaciones prolongadas. En segundo lugar, es lo suficientemente flexible para facilitar la evaluación de nuevos enfoques y ajustes a los rápidos desarrollos en el campo de la gobernanza. Por último, la legislación blanda brinda una mayor oportunidad para el enfoque de múltiples partes interesadas que cualquier otro enfoque internacional legal restringido a los estados y organizaciones internacionales.

Ius cogens

El *Ius cogens* está definido en el Convenio de Viena sobre el Derecho de los Tratados[8] en el artículo 53 como una «norma aceptada y reconocida por la comunidad internacional de Estados en su conjunto, como norma que no admite acuerdo en contrario y que solo puede ser modificada por una norma ulterior de derecho internacional general que tenga el mismo carácter». El profesor Ian Brownlie, exbecario de All Souls College en la Universidad de Oxford, enumeró los siguiente ejemplos de normas *ius cogens*:

- La prohibición del uso de la fuerza.
- La ley de genocidio.
- El principio de no discriminación racial.
- Crímenes de lesa humanidad.
- Reglas que prohíben el tráfico de esclavos y la piratería.[9]

En la gobernanza de Internet, el *ius cogens* podría ser relevante en el abordaje de actividades en línea que promuevan y/o faciliten la organización de actividades prohibidas por el *ius cogens* (como el genocidio, la discriminación racial, la esclavitud, etc.).

Jurisdicción

La jurisdicción es la autoridad que tiene la corte y los órganos estatales para resolver casos judiciales. La relación entre la jurisdicción y la Internet ha sido ambigua, ya que la jurisdicción depende predominantemente de la división geográfica de los territorios nacionales del mundo. Cada estado tiene el derecho soberano de ejercer su jurisdicción sobre su territorio. Sin embargo, la Internet facilita considerablemente el intercambio transfronterizo, difícil (aunque no imposible) de monitorear mediante los mecanismos gubernamentales tradicionales. La cuestión de la jurisdicción sobre Internet pone de relieve uno de los dilemas centrales asociados con la gobernanza de Internet: ¿Cómo es posible anclar la Internet dentro de la geografía política y legal existente?[10]

En los últimos años, los tribunales han enfrentado un creciente número de casos con un fuerte elemento jurisdiccional. Algunos de los ejemplos que se destacan son: las sentencias sobre el derecho al olvido, los casos en que las autoridades solicitan datos ubicados en otras jurisdicciones, y la anulación del marco Safe Harbour. En estos casos, el largo brazo de la jurisdicción se extendió más allá de los territorios nacionales o de la UE.

Varios de estos casos fueron resueltos en tribunales europeos, y tuvieron numerosas consecuencias:

- Los tribunales europeos están imponiendo su jurisdicción sobre un gran número de casos que involucran a compañías de EE. UU.
- El rol de los reguladores en Europa, especialmente de las autoridades de protección de datos, es más prominente.

- La jurisprudencia global concerniente a asuntos de Internet se ve moldeada cada vez más por las cortes europeas.

Principios de jurisdicción

Hay tres consideraciones importantes al momento de tomar decisiones sobre la jurisdicción:

- ¿Qué tribunal o autoridad estatal tiene la competencia adecuada? (Jurisdicción procesal)
- ¿Qué reglas deberían aplicar? (Jurisdicción sustantiva)
- ¿Cómo deberían implementarse los fallos judiciales? (Jurisdicción de aplicación)

Los siguientes criterios establecen la jurisdicción en casos particulares:

- Principio territorial – el derecho del estado a gobernar a la gente y a la propiedad dentro de su territorio.
- Principio de personalidad – el derecho del estado a gobernar a sus ciudadanos dondequiera que estén (principio de nacionalidad).
- Principio de efectos – el derecho del estado de gobernar sobre los efectos económicos y legales en su territorio, provenientes de actividades llevadas a cabo en el exterior.

Otro principio importante que introdujo el derecho internacional moderno es el de la jurisdicción universal.[11] «El concepto de jurisdicción universal en su sentido más amplio es el poder que tiene un estado para castigar ciertos crímenes, dondequiera y por quienquiera que hayan sido cometidos, sin necesidad de tener una conexión con el territorio, nacionalidad, o interés estatal especial».[12]

La jurisdicción universal cubre crímenes, tales como delitos de privacidad, crímenes de guerra, y genocidio. Sin embargo, la Internet ha introducido funcionalmente la jurisdicción universal en un conjunto mucho más amplio de casos basados en el principio de accesibilidad. Según este principio, acceder a Internet desde un país determinado es una base suficiente para que aplique la jurisdicción de este país. Este principio apareció en la corte francesa en el caso de Yahoo!,[13] así como también en el TJUE en los casos de eData[14] y Pinckney[15]. La posibilidad de invocar la jurisdicción mediante un criterio limitado como el acceso a Internet podría dar comienzo a varios problemas, incluido el foro de conveniencia. A saber, el procedimiento judicial podría iniciarse desde cualquier país con acceso a Internet.

Conflicto de jurisdicción

El conflicto de jurisdicción surge cuando más de un estado reclama la jurisdicción de un caso legal en particular. Esto sucede comúnmente cuando un caso judicial involucra un componente extraterritorial (por ejemplo, individuos de distintos estados, o transacciones internacionales). La jurisdicción pertinente se establece sobre la base de uno de los siguientes elementos: territorialidad, nacionalidad, o efecto de acción. Al publicar contenido o interactuar en Internet, resulta difícil saber qué ley nacional, llegado el caso, podría ser quebrantada. En este contexto, casi toda la actividad de Internet cuenta con un aspecto

internacional que podría involucrar a múltiples jurisdicciones o resultar en el denominado efecto colateral.[16]

Jurisdicción y acceso al contenido

Uno de los primeros y más citados casos que ejemplifican el problema de las múltiples jurisdicciones es el de Yahoo! en Francia. Fue suscitado por una violación al derecho francés, que prohíbe la exhibición y venta de objetos nazis, aunque el sitio web que proporcionaba estos productos – el sitio de subastas de Yahoo.com – tenía su *host* en EE. UU., país en donde la exposición de dichos materiales es legal. El caso judicial se resolvió mediante una solución técnica (*software* de geolocalización y filtrado de acceso). Forzaron a Yahoo! a identificar a los usuarios que habían accedido al sitio desde Francia para bloquear sus accesos a las páginas que exhibieran material nazi.[17]

De manera similar, la sentencia sobre el derecho al olvido (Google *et al.* v Mario Costeja Gonzalez *et al.*) impuso, a los motores de búsqueda, la obligación de considerar las solicitudes de los usuarios europeos de eliminar ciertos resultados de las búsquedas. La sentencia también tomó forma sobre la base de los fallos sobre protección de datos de autoridades europeas. Mediante la aplicación de un razonamiento similar al que se usó en el caso Yahoo!, el regulador francés, por ejemplo, falló[18] que la supresión de la lista de resultados debería aplicarse en Google de manera global, y no solo en los países europeos y sus extensiones (como .fr, .es, y .uk).

Jurisdicción y protección de datos

La protección de los datos personales de los ciudadanos de la UE almacenados en lugares no europeos contribuyó en uno de los casos más polémicos de los últimos años. En 2013, Maximilian Schrems, ciudadano de Austria, presentó una denuncia en la que pedía que el Comisionado de Protección de Datos de Irlanda prohibiera a Facebook transferir sus datos personales a EE. UU. Schrems argumentó que EE. UU. no brindaba una adecuada protección a los datos de los usuarios, ya que estos quedan sometidos a la vigilancia masiva bajo las leyes de EE. UU. El Comisionado denegó esta petición, y Schrems impugnó esa decisión en la corte. El caso llegó al TJUE, que reguló que el Marco Safe Harbour que rige la transferencia de los datos personales entre la UE y EE. UU. carecía de validez.[19] Esto llevó a que el acuerdo Safe Harbour fuera reemplazado por el Marco del Escudo de la Privacidad entre la UE y EE. UU.

Consulte la Sección 8 para saber más sobre Safe Harbour y el Escudo de la Privacidad.

Las consideraciones sobre la protección de datos contribuyeron en dos desarrollos. El primero tiene que ver con que varias compañías trasladaron sus centros de datos y sus funciones de tratamiento de datos a jurisdicciones que son conocidas por contar con un enfoque normativo más relajado, como es el notable caso de Irlanda. A pesar de que esto no les ha ahorrado procedimientos judiciales a las compañías, una sentencia de 2016, que involucra a Microsoft, confirmó que EE. UU. no puede utilizar una orden de registro local para obtener acceso a los datos almacenados en Irlanda.[20]

El segundo tiene que ver con que algunos países, como China y Rusia, promulgaron leyes que requieren que los datos de los usuarios estén almacenados localmente. El almacenamiento de datos en servidores ubicados en el territorio nacional es un pilar importante de la política china hacia el logro de la soberanía cibernética.

Jurisdicción y términos de uso

La disposición de la jurisdicción en los términos de uso de las compañías también fueron el centro de atención en muchos fallos de las cortes, en los que muchas veces la compañía Facebook estaba involucrada.

Un caso relevante involucró a un profesor francés, cuya cuenta de Facebook fue suspendida tras haber publicado imágenes de una pintura de desnudos que se encuentra en el Musée d'Orsay. El Tribunal de Apelaciones de París sentenció[21] que Facebook debía ser demandado en Francia, al rechazar el argumento de esta red social sobre que sus términos de uso indican que California tiene jurisdicción. El tribunal francés abrió el camino a otras demandas contra la compañía fuera de la jurisdicción estadounidense.

En junio de 2016, un tribunal israelí sentenció que era nula la cláusula en los términos de uso de Facebook que requiere que todas las demandas se lleven a cabo en tribunales de California, y aprobó un caso de juicio colectivo contra Facebook.[22] El caso alegó que Facebook había violado la privacidad de sus usuarios al usar publicaciones privadas para determinar el tipo de publicidad que deberían ver, sin obtener su consentimiento previo.

Además de las soluciones técnicas (geolocalización y técnicas de filtrado), otros enfoques para resolver el conflicto de la jurisdicción incluyen la armonización de leyes nacionales y el uso de mecanismos de Resolución Alternativa de Conflictos.

La armonización de leyes nacionales

La armonización de leyes nacionales podría resultar en el establecimiento de un conjunto de reglas compatibles a nivel mundial. Mediante la implementación de reglas armonizadas, la cuestión de la jurisdicción pierde relevancia. La armonización se puede lograr en áreas en las que ya existe un alto nivel de consenso mundial, por ejemplo, con respecto al contenido de abuso sexual de menores, la privacidad, la esclavitud, y el terrorismo. También hay convergencia en otros asuntos, como en la ciberdelincuencia. No obstante, en algunos campos, como las políticas de contenido, no es muy probable llegar a un acuerdo mundial sobre las reglas básicas, ya que las diferencias culturales continúan chocando en el entorno en línea de una manera más notable que fuera de línea.[23]

Otra posible consecuencia de la falta de armonización es la migración de contenido hacia países con niveles de reglamentación más bajos. En términos de la analogía del Derecho del Mar, algunos países podrían convertirse en «banderas de conveniencia» para el contenido en línea.

www.igbook.info/jurisdiction

Resolución alternativa de conflictos

La Resolución Alternativa de Conflictos (ADR, por sus siglas en inglés) es un mecanismo disponible vigente en lugar de los tribunales tradicionales. Las herramientas ADR son el arbitraje y la mediación. La resolución de conflictos en línea usa la Internet y la tecnología en el proceso de resolución de conflictos.

Cuando se trata de casos de Internet, estos mecanismos – en particular, el arbitraje – se utilizan frecuentemente para cerrar la brecha provocada por la incapacidad del derecho internacional privado actual para lidiar con tantos casos legales de la Internet. Un ejemplo es la UDRP (Política Uniforme para la Resolución de Disputas), desarrollada por OMPI y ICANN como el principal procedimiento de resolución de conflictos en temas relacionados con la registración de nombres de dominio.

En el arbitraje, uno o más individuos escogidos por los disputantes toman las decisiones. Usualmente, el mecanismo se explica en un contrato privado, que también detalla información como el lugar del arbitraje, los procedimientos, y la elección de la legislación. El arbitraje internacional dentro del sector comercial cuenta con una larga tradición.

El Cuadro 2 muestra un resumen corto de las principales diferencias entre los sistemas tradicionales de tribunales y el arbitraje.

Cuadro 2. Diferencias entre los tribunales y el arbitraje.

Elementos	Tribunales	Arbitraje
Organización	Establecidos mediante leyes nacionales y tratados	Arbitrajes permanentes y ad hoc (establecidos y / o seleccionados por las partes)
Derecho aplicable	La ley del tribunal – (el juez decide sobre la ley aplicable)	Las partes pueden escoger la legislación; en caso contrario, se utiliza la ley indicada en el contrato; si no existe tal indicación, se utiliza la ley del órgano de arbitraje
Procedimiento	Los procedimientos judiciales de resuelven mediante leyes/tratados	Resuelto por las partes – provisional, ad hoc Resueltos por la regulación del órgano de arbitraje – permanente
Aplicación	Aplicado por las autoridades nacionales	Aplicado de conformidad con el acuerdo de arbitraje y la Convención de Nueva York

En comparación con los tribunales tradicionales, el arbitraje ofrece muchas ventajas: mayor flexibilidad, gastos más bajos, rapidez, elección de la jurisdicción, y una aplicación más fácil de las sentencias arbitrales extranjeras.

Una de las ventajas más importantes del arbitraje es que elimina el potencial conflicto sobre la jurisdicción. El arbitraje brinda ventajas especiales en cuanto a una de las tareas

más difíciles en los casos judiciales de Internet: la aplicación de las sentencias judiciales. La Convención sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales Extranjeras[24] regula la aplicación de los fallos arbitrales. Según esta convención, los tribunales nacionales están obligados a ejecutar las sentencias arbitrales. A menudo es más fácil aplicar las sentencias arbitrales en países extranjeros usando el régimen de la Convención de Nueva York en lugar de ejecutar las sentencias de los tribunales extranjeros.

La mayor limitación que presenta el arbitraje es que no puede abordar temas de interés público superior como la protección de derechos humanos; estos temas requieren la intervención de tribunales establecidos por el estado. También surgen otras limitaciones:

- Debido a que el arbitraje usualmente se establece mediante previo acuerdo, no cubre una amplia área de temas cuando no existe un acuerdo entre las partes de antemano (difamación, varios tipos de responsabilidades, ciberdelincuencia).

- Muchos consideran que la práctica actual de incorporar una cláusula de arbitraje a los contratos comunes es desfavorable para la parte más débil en el contrato (que, por lo general, es el usuario de Internet o el cliente del comercio electrónico).

- Algunos se preocupan por que el arbitraje extienda la legislación basada en precedentes (el sistema legal de EE. UU. y el Reino Unido) a nivel global y que suprima gradualmente a otros sistemas legales. En el caso del comercio electrónico, esto podría resultar más aceptable, dado el alto nivel de armonización presente en las reglas del derecho comercial en ley precedente. Sin embargo, esta extensión es mucho más delicada cuando se trata de temas socioculturales como el contenido de Internet, en donde el sistema jurídico nacional refleja un contexto cultural específico.

El arbitraje se ha utilizado ampliamente en los conflictos comerciales. Existe un sistema bien elaborado de reglas e instituciones que abordan los conflictos comerciales. El principal instrumento internacional es la Ley Modelo sobre Conciliación Comercial Internacional de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI).[25] Los arbitrajes internacionales más importantes están generalmente unidos a las cámaras de comercio.

ADR, ODR, y la Internet

El arbitraje y otros sistemas de Resolución Alternativa de Conflictos se usan de manera extensiva en casos relacionados con Internet, y la UDRP mencionada anteriormente es un ejemplo de esto. Desde el comienzo de sus tareas bajo la UDRP en diciembre de 1999, el arbitraje de la OMPI y el Centro de Mediación ha administrado más de 35.000 casos de nombres de dominios.[26]

La UDRP se estipula de antemano como el mecanismo de resolución de conflictos en todos los contratos que tengan que ver con la registración de nombres de dominio gTLD (por ejemplo, .com, .edu, .org, .net) y también de algunos ccTLD. Un aspecto especial del arbitraje es que sus fallos siempre se aplican directamente mediante cambios relativos al nombre de dominio en disputa (la cancelación del nombre de dominio, o la transferencia de la registración del nombre de dominio al demandante), sin tener que recurrir a su ejecución mediante los tribunales nacionales.

La UE introdujo una nueva plataforma de resolución de conflictos en 2016. La plataforma de Resolución de Litigios en línea (ODR, por sus siglas en inglés), en funcionamiento desde

febrero de 2016, tiene como finalidad ayudar a los consumidores y comerciantes a resolver sus disputas en línea, con respecto a adquisiciones en línea nacionales o transfronterizas.[27]

Una serie de compañías de Internet (por ejemplo, Google, Facebook, y Twitter) también desarrollaron sus propios mecanismos. Tras la sentencia del TJUE sobre el derecho al olvido, Google estableció un mecanismo especial que permite a las personas solicitar la remoción de sitios web de los resultados de búsqueda. De mayo de 2014 a octubre de 2016, Google recibió más de 575.000 solicitudes de remoción.[28]

A partir de esta práctica de resolución de disputas, surgen varias preguntas: Las compañías privadas, ¿deberían brindar mecanismos de resolución de conflictos? ¿Cuáles son las reglas procesales y sustantivas por aplicar? ¿Cómo se puede asegurar el acceso a estos mecanismos a los usuarios de Internet afectados?

www.igbook.info/arbitration

Derechos de propiedad intelectual

En la economía mundial, el conocimiento y las ideas son recursos clave. La protección del conocimiento y la expresión de las ideas, mediante los IPR se ha convertido en uno de los temas de mayor predominancia en el debate de la gobernanza de Internet, y cuenta con un fuerte componente orientado al desarrollo. Los IPR se vieron afectados por el desarrollo de Internet, más que nada mediante la digitalización del conocimiento y la información, así como también a causa de las nuevas posibilidades para su manipulación. Los IPR relacionados con la Internet incluyen: el derecho de autor, las marcas comerciales, y las patentes. Otros IPR abarcan los diseños, modelos de utilidad, secretos comerciales, indicaciones geográficas, y variedades vegetales.

© Derecho de autor

El derecho de autor (*copyright*) es un concepto legal que describe el derecho que tienen los creadores sobre sus obras originales. Únicamente protege la expresión de una idea cuando se materializa de alguna forma, como en un libro, CD, o archivo de computadora. La idea en sí misma no se encuentra protegida por este derecho. En la práctica, sin embargo, resulta difícil realizar una clara distinción entre la idea y su expresión.

El régimen del derecho de autor siguió muy de cerca la evolución de la tecnología. Cada invención nueva, como la imprenta, la radio, la televisión, y la videograbadora, afectó tanto la forma como la aplicación de las reglas de derecho de autor. La Internet no es la excepción. El concepto tradicional del derecho de autor se vio desafiado de muchas maneras, desde aquellas simples prácticas de cortar y pegar fragmentos de textos desde la web hasta actividades más complejas, como la distribución masiva de música y vídeos a través de Internet.

La Internet también empodera a los titulares de los derechos de autor al brindarles herramientas técnicas más poderosas para proteger y monitorear el uso del material protegido por los derechos de autor. Estos desarrollos pusieron en peligro el delicado balance entre

Figura 17. Derecho de autor

los derechos de los autores y el interés público, lo que representa la base de la legislación sobre los derechos de autor (Figura 17).

Hasta el momento, los titulares de los derechos de autor, representados por las más reconocidas compañías discográficas y de multimedia, han protegido de manera muy activa sus IPR. El interés público se considera a menudo algo muy poco percibido y sin la protección suficiente. Sin embargo, esto fue cambiando gradualmente, gracias a numerosas iniciativas globales que se centran en el libre acceso al conocimiento y la información (por ejemplo, Creative Commons).

La situación actual

Protección de los derechos de autor más estricta a nivel nacional e internacional

Las industrias discográficas y del entretenimiento estuvieron ejerciendo presión a nivel nacional e internacional para fortalecer la protección de los derechos de autor. A nivel internacional, se introdujo la protección de las piezas digitales en el Tratado de la OMPI sobre Derecho de Autor[29] (1996). Este tratado también contiene disposiciones para ajustar más el régimen de protección del derecho de autor, como disposiciones más estrictas para las limitaciones de los derechos exclusivos de los autores, la prohibición de burlar la protección tecnológica del derecho de autor, y otras medidas acordes. A nivel regional, las disposiciones IPR en el Tratado de Asociación Transpacífico, un acuerdo comercial entre 12 países de la cuenca del Pacífico, contiene duras reglas de aplicación además de que aumenta el lapso de la protección del derecho de autor.[30] En EE. UU., se introdujo una protección más estricta mediante la DMCA[31] de 1998.

Varias reglamentaciones propuestas a nivel nacional e internacional están destinadas a la ejecución de un control más estricto, obligando a los intermediarios a filtrar o monitorear la diseminación del contenido protegido por el derecho de autor. Estas propuestas provocaron una fuerte protesta por parte del público, lo que detuvo su promulgación. En 2011, en EE. UU., se presentaron dos proyectos de ley: la ley SOPA[32] y la ley PROTECT IP

(PIPA).[33] Estos proyectos proporcionaban nuevos medios para la lucha contra la piratería en línea, e incluían el bloqueo al acceso a sitios web en violación y la prohibición de que los motores de búsqueda condujeran a dichos sitios. Tras las protestas en su contra, ambas fueron pospuestas. A nivel internacional, la ley ACTA[34] intentó hacer frente a las violaciones de los IPR de una manera que puede haber abierto la posibilidad de la ejecución privada (compañías) y la acción policial. Luego de fuertes protestas en Europa, el Parlamento Europeo votó en contra de la ley ACTA.

Estas acciones normativas recibieron duras críticas por parte de académicos y grupos de libertades civiles sobre la base de los derechos humanos y las libertades. Los usuarios de Internet individuales se unieron a protestas en línea y fuera de línea.[35]

Software contra la violación del derecho de autor

Los infractores del derecho de autor acuden a herramientas de *software*, por ejemplo, para distribuir música y vídeos de manera ilícita en línea. Los defensores de los derechos de autor también acuden a ellas. Tradicionalmente, las autoridades estatales y el sector comercial llevaban a cabo sus responsabilidades en este ámbito por medio de mecanismos jurídicos. Sin embargo, va en aumento el uso de herramientas de *software* «alternativas» por parte del sector comercial contra los infractores del derecho de autor.

Algunas tácticas basadas en *software* que usan o defienden las compañías discográficas/de entretenimiento están destinadas a proteger sus derechos de autor:

- Un troyano redirige a los usuarios adonde pueden comprar de manera lícita las obras protegidas por el derecho de autor (por ejemplo, una canción) que estaban intentando descargar.
- El software de congelación bloquea la computadora por un momento y muestra una advertencia sobre la descarga de contenido pirateado.
- El escaneo del disco duro busca e intenta eliminar cualquier archivo pirateado encontrado.
- La interdicción evita el acceso a Internet a aquellos que tratan de descargar o compartir contenido pirateado.

Algunos consideran que estas medidas son ilegales.[36] La pregunta es si las compañías que usan estas medidas de autoayuda quebrantan la ley.

Tecnologías para la gestión de derechos digitales

En la búsqueda de un enfoque a largo plazo y más estructurado, el sector comercial introdujo varias tecnologías para la gestión del acceso a los materiales protegidos por el derecho de autor. Microsoft introdujo un *software* de gestión de derechos digitales para administrar la descarga de archivos de sonido, películas, y otros materiales protegidos. Otros sistemas similares fueron los desarrollados por Xerox (ContentGuard), Philips, y Sony (InterTrust).

El uso de herramientas tecnológicas para la protección del derecho de autor encuentra su fundamento jurídico en el Tratado de la OMPI sobre el Derecho de Autor y en la ley DMCA. Además, la DMCA penaliza la actividad destinada a eludir la protección tecnológica de los materiales de derecho de autor.

Los asuntos

Modificar los mecanismos de protección del derecho de autor existentes o desarrollar nuevos

¿Cómo deberían ajustarse los mecanismos de protección del derecho de autor para que reflejen los profundos cambios provocados por los desarrollos de las TIC y la Internet? Una respuesta sugerida por el gobierno de EE. UU. en el Libro Blanco sobre Propiedad Intelectual y la Infraestructura Nacional[37] es que solo se necesitan pequeñas modificaciones en la regulación existente, principalmente mediante la «desmaterialización» de los conceptos de derecho de autor de «fijación», «distribución», «transmisión», y «publicación». Se siguió este enfoque en los principales tratados internacionales sobre el derecho de autor, como el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (TRIPS, por sus siglas en inglés) y el Tratado de la OMPI sobre el Derecho de Autor.

Sin embargo, una opinión opuesta argumenta que los cambios en el sistema legal deben ser de fondo, ya que el derecho de autor en la era digital ya no se refiere simplemente al «derecho a evitar la copia» sino también al «derecho a evitar el acceso». Finalmente, gracias a las aun más grandes posibilidades técnicas de restricción de acceso a material digital, la pregunta es si la protección del derecho de autor es realmente necesaria. Queda por ver cómo proteger el interés público, la otra parte de la ecuación del derecho de autor.

Protección del interés público – el uso legítimo de los materiales protegidos por el derecho de autor

El derecho de autor se diseñó originalmente para incentivar la creatividad y la invención. Combinaba dos elementos: la protección de los derechos del autor y la protección del interés público. El desafío más importante era el de estipular cómo accedería el público a los materiales protegidos por este derecho para mejorar la creatividad, el conocimiento, y el bienestar mundial. Desde la perspectiva operacional, el concepto de «uso legítimo» de los materiales protegidos asegura la protección del interés público.[38]

Derecho de autor y desarrollo

Mientras más estricta es la aplicación del derecho de autor, más afectados se ven los países en vías de desarrollo. La Internet representa una poderosa herramienta para la participación en el intercambio académico y científico global para los investigadores, estudiantes, y otras personas de países en desarrollo. Un régimen más restrictivo podría generar un impacto negativo en el desarrollo de las capacidades humanas en estos países. Otro aspecto es la creciente digitalización de sus trabajos culturales y artísticos. Si pensamos en el panorama más paradójico, los países en vías de desarrollo podrían terminar pagando su herencia cultural y artística si las compañías de entretenimiento y de comunicación se adueñan de ella, la digitalizan, y la reempacan.

OMPI y OMC

Existen dos principales regímenes internacionales para los IPR. La OMPI gestiona el régimen de los IPR que se basa en los convenios de Berna y París. El régimen de la OMC está basado en el TRIPS. La transición de la coordinación internacional de los IPR desde la OMPI hacia la OMC tenía como finalidad fortalecer la protección de los derechos, especialmente en el campo de la aplicación de la ley.

Algunos países en desarrollo se preocuparon por esto. Su preocupación es que los estrictos mecanismos de aplicación de la OMC podrían reducir el espacio de maniobra de los países en desarrollo y la posibilidad de equilibrar las necesidades de desarrollo con la protección internacional de los IPR. Hasta ahora, el foco primordial de la OMC y el TRIPS estuvo en las variadas interpretaciones de los IPR para los productos farmacéuticos. Es muy probable que los debates se extiendan a los IPR y la Internet.

www.igbook.info/copyright

Marcas registradas

Una marca registrada es un símbolo, o una o más palabras legalmente registradas o establecidas por su uso que representa a una compañía o un producto. La relevancia de las marcas registradas con respecto a Internet se debe, más que nada, a la registración de los nombres de dominio. En los primeros días del desarrollo de Internet, la registración de nombres de dominio se hacía por orden de llegada. Esto llevó a la ciberocupación: la práctica de registrar nombres de compañías y después vender ese nombre a un precio más elevado.

Esta situación obligó al sector comercial a ubicar la cuestión de la protección de las marcas comerciales en el centro de la reforma de la gobernanza de Internet, lo que condujo a la creación de ICANN en 1998. En el Libro Blanco sobre la Gestión de los Nombres y Direcciones de Internet, el gobierno de EE. UU. solicitó el desarrollo y la implementación de un mecanismo para la protección de marcas registradas en el campo de los nombres de dominio.[39] Poco tiempo después de su formación, ICANN introdujo la UDRP.[40]

Las inquietudes de las marcas comerciales ganaron más atención cuando el espacio del nombre de dominio se extendió al introducir nuevos gTLD como «.doctor», «.lawyer», «.berlin», etc. Un ejemplo de esta polémica es la aplicación del gTLD «.amazon». La compañía de Internet Amazon se postuló para registrar «.amazon», como el titular de la marca para este nombre. Los países de la cuenca del Amazonas protestaron ante el GAC de ICANN, señalando que ese nombre hace referencia a una zona geográfica que es importante para la región, y que no se le debía asignar a la compañía el uso exclusivo de ese gTLD. Sobre la base de las recomendaciones del GAC, la Junta de ICANN rechazó esta aplicación en mayo de 2014, decisión que fue impugnada luego por Amazon, mediante el Proceso de Revisión Independiente (IRP, por sus siglas en inglés) de ICANN. Hasta octubre de 2016, el caso seguía abierto, con el IRP en marcha, y una audiencia programada en principio para febrero-marzo de 2017.[41]

www.igbook.info/trademarks

Patentes

Una patente le confiere a su titular el derecho exclusivo de impedir que otros produzcan, usen, o vendan un invento. Tradicionalmente, las patentes protegen un nuevo proceso o producto de naturaleza principalmente técnica o productiva. Hace poco se comenzaron a otorgar patentes para *software*.

Debido a la continua evolución de las tecnologías de Internet, cada vez más compañías solicitan patentes (abarcando las tecnologías en el campo del VoIP, la IoT, etc.). Este es especialmente el caso en EE. UU., en donde más registraciones de patentes también derivan en más casos judiciales entre las compañías, lo que implica grandes sumas de dinero. A modo de ejemplo, en septiembre de 2016, en un caso que había comenzado en 2010, un juez del estado de Texas de EE. UU. ordenó que Apple pagara $302,4 millones de dólares a otra compañía estadounidense, por violar las patentes que cubrían comunicaciones móviles e informáticas seguras.[42]

Algunas patentes fueron otorgadas con propósitos comerciales, y surgieron polémicas sobre algunas de ellas, como la solicitud de British Telecom para cobrar tarifas de licencia por el uso de los enlaces de hipertexto que patentó en la década de 1980. En agosto de 2002, el caso fue sobreseído.[43] Si British Telecom hubiera ganado el caso, los usuarios de Internet habrían tenido que pagar una tarifa cada vez que crearan o usaran un enlace de hipertexto.

En Europa y otras regiones, otorgar patentes para *software* es una acción un poco compleja. Como explica la Oficina Europea de Patentes, «en virtud del Convenio de la Patente Europea (CPE), un programa de ordenador reivindicado "como tal" no es una invención patentable [...]. Pueden concederse patentes para invenciones implementadas en ordenador que resuelvan un problema técnico de forma inventiva».[44]

Derecho laboral

La Internet cambió la manera en la que trabajamos. El concepto del teletrabajo ganó relevancia, junto con el crecimiento de una serie de trabajos temporarios y de corto plazo. El término «permatemp» fue acuñado por empleados que trabajan por largos periodos de tiempo, sobre la base de contratos temporales que se renuevan con regularidad. Esto hace que el nivel de protección social de la fuerza de trabajo se reduzca (Figura 18).

Los nuevos modelos laborales, como los modelos de trabajo por demanda y los trabajadores independientes, son un desarrollo más reciente en los modelos comerciales moldeados por Uber, Amazon, y otras compañías de Internet. En el proceso, surgieron muchas preguntas con estos modelos nuevos. Por ejemplo, los conductores de Uber, ¿son trabajadores independientes o empleados de Uber? Diferentes puntos de vista se esparcieron por todos los estados de EE. UU.: las autoridades de California[45] y Oregón[46] consideran que los conductores son empleados de Uber, mientras que [47]Florida los califica como trabajadores independientes.

En el campo del derecho laboral, la privacidad en el lugar de trabajo es un tema importante. ¿Se le permite a un empleador monitorear el uso de Internet de los empleados (como el contenido de los correos electrónicos y el acceso a sitios web? Poco a poco, la jurisprudencia se hace más tangible en este campo.

Si bien una resolución de 2007 del Tribunal Europeo de Derechos Humanos (TEDH) declaró que monitorear el correo electrónico o el uso de Internet de un empleado en el lugar de trabajo representaba una violación al derecho humano de este,[48] una resolución de 2016 del mismo tribunal sentenció que los empleadores pueden leer las comunicaciones privadas de los empleados que tuvieran lugar durante las horas de oficina. El fundamento del tribunal en el caso Bărbulescu vs Rumania (enero de 2016) fue que no era ilógico que un empleador quisiera verificar que sus empleados completen sus tareas durante las horas laborales. Sin embargo, el empleador debe notificar previamente a sus empleados sobre las

Figura 18. Derecho laboral

actividades de monitoreo. En Dinamarca, los tribunales tuvieron que lidiar con un caso que involucraba el despido de un empleado por haber enviado correos electrónicos privados e ingresado a salones de chat de índole sexual. El tribunal determinó que el despido era ilícito, ya que el empleador no contaba con una política de uso de Internet que prohibiera el uso de Internet no oficial. La sentencia del TEDH de Bărbulescu vs Rumanía también pone de relieve la necesidad de contar con una política: «Se debe adoptar una política comprensiva sobre el uso de Internet en el lugar de trabajo, que incluya reglas específicas sobre el uso del correo electrónico, la mensajería instantánea, las redes sociales, los blogs, y la navegación de la web. Aunque dicha política puede estar ajustada a las necesidades de cada empresa en su totalidad y cada sector de la infraestructura empresarial en particular, los derechos y obligaciones de los empleados deberían estar descriptos claramente, mediante reglas transparentes sobre cómo se puede usar la Internet, cómo se lleva a cabo el monitoreo, como se protegen, usan y destruyen los datos, y quién tiene acceso a ellos».[49]

Otro motivo de preocupación que surge del creciente uso de las redes sociales es la delimitación entre la vida privada y la vida laboral. En casos recientes[50], el comportamiento y los comentarios de los empleados en las redes sociales eran variados, desde el lugar de trabajo y los compañeros de oficina hasta las estrategias y productos del empleador, considerados como opiniones personales (y privadas), pero que pueden afectar significativamente la imagen y reputación de la compañía y los colegas.

El derecho laboral ha sido, tradicionalmente, un asunto nacional. Sin embargo, la globalización en general y la Internet en particular dieron lugar a la internacionalización de los asuntos laborales. Con el creciente número de personas que trabajan para entidades del extranjero y que interactúan con equipos de trabajo mundialmente, emerge la necesidad de implementar los mecanismos normativos internacionales pertinentes. Este aspecto fue reconocido en la Declaración de Principios de la CMSI, que, en el párrafo 47, pide el respeto de todas las normas internacionales concernientes al campo del mercado laboral TIC.[51]

www.igbook.info/labourlaw

Intermediarios

Los intermediarios[52] cumplen un rol crucial en la garantía del funcionamiento de Internet. Los intermediarios son los PSI (que aseguran la conexión entre los usuarios finales), y también los proveedores de servicios como el *hosting* en línea, los motores de búsqueda, y las plataformas de redes sociales.

Gracias a su rol en la facilitación, y la transmisión y disponibilidad del contenido en línea, los intermediarios están solicitando cada vez más asistir en la aplicación de las normas jurídicas en áreas como la violación del derecho de autor, el correo no deseado, y el derecho al olvido. Esto dio comienzo a debates extensos sobre si los intermediarios son los responsables o si deberían responsabilizarse por el contenido en línea al que ellos dan acceso.

A nivel nacional, los PSI son a menudo la manera más directa para que los gobiernos y las autoridades de aplicación de la ley hagan cumplir las reglas jurídicas en línea.

Típicamente, los *hosts* de contenido en línea, los operadores de motores de búsqueda, y las plataformas de redes sociales actúan como conductos para el contenido, o representan puentes entre el contenido y los usuarios. Aunque tienen su sede central en un país (algunos tienen sedes regionales), su alcance y base de usuarios probablemente pueda ser global, y como consecuencia, por lo general quedan expuestos a la jurisdicción de múltiples países.

La responsabilidad de intermediarios se discute con frecuencia en las reuniones del IGF y otros foros. La OCDE incluye el rol de los intermediarios entre sus 14 principios para la elaboración de políticas de Internet,[53] mientras que el CdE estableció un Comité de expertos sobre intermediarios de Internet (MSI-NET), encargado de la preparación de un conjunto de propuestas sobre los roles y las responsabilidades de los intermediarios. La UNESCO exploró el rol de mediación que desempeñan los intermediarios de Internet entre los autores de contenido y los usuarios de Internet, así como también su impacto en la libertad de expresión y derechos fundamentales asociados, como la privacidad.[54]

Los asuntos

La responsabilidad de los intermediarios en la violación de los derechos de autor

En general, los marcos jurídicos que abordan la responsabilidad de los intermediarios incluyen el principio de que un intermediario de Internet no puede considerarse culpable por alojar contenido que viole los derechos de autor, siempre y cuando no sean conscientes de dicha violación. Este es el enfoque de, por ejemplo, la ley DMCA y las directivas de la UE,[55] que eximen al proveedor de servicios de la responsabilidad de la información transmitida o almacenada por encargo de sus usuarios.

La principal diferencia entre los distintos sistemas jurídicos yace en la acción legal que se toma luego de que el intermediario toma conocimiento de que el material que aloja viola el derecho de autor. El derecho de EE. UU. y el de la UE exigen que los proveedores de servicios sigan el procedimiento de «detección y eliminación».[56] El derecho japonés toma un enfoque más equilibrado, mediante un procedimiento de detección y eliminación que le da la oportunidad al usuario del material de impugnar la solicitud de remoción. Ambas soluciones les proporcionan algo de confort a los intermediarios, gracias a que no se les impone ninguna sanción, pero también los transforma en potenciales jueces de contenido[57] y el

problema no queda completamente resuelto, ya que el contenido en cuestión puede ser trasladado a otra ubicación en línea.

La jurisprudencia, en general, apoya el enfoque de imponer una responsabilidad limitada sobre los intermediarios. Algunos de los casos más importantes en los que los PSI fueron absueltos de toda responsabilidad por alojar materiales que violaban la ley de derecho de autor son el caso de Cienciología (Países Bajos),[58] RIAA vs Verizon (EE. UU.),[59] SOCAN vs CAIP (Canadá),[60] y Scarlet vs SABAM (Bélgica).[61] Una sentencia más matizada emitida por la TJUE en septiembre de 2016, en el asunto GS Media BV vs Sanoma Media Netherlands BV y otros, establece que los operadores de los sitios web conectados a materiales que violan el derecho autor pueden ser declarados culpables de violación del derecho de autor, siempre y cuando los operadores hayan sabido o podrían haber pensado que los materiales representaban una violación. Según el Tribunal, se presume que los operadores saben sobre esta violación si los enlaces se brindan «en búsqueda de ganancias financieras».[62]

Sin embargo, los últimos años presenciaron una presión incrementada sobre los intermediarios por el manejo de los temas del derecho de autor, ya que su posición como guardianes entre los usuarios finales y el contenido de Internet los sitúa en el mejor lugar para controlar el acceso. Este argumento se tuvo en cuenta en la promoción de disposiciones legales como la ley Hadopi[63] en Francia, que obliga a los PSI a intervenir en caso de que haya sospechas de violaciones del derecho de autor.

El rol de los intermediarios en las políticas actuales

Bajo una creciente presión oficial, los PSI, los proveedores de servicios de *hosting*, y los operadores de motores de búsqueda y plataformas de redes sociales están poco a poco, aunque a regañadientes, involucrándose en las políticas de contenido (por ejemplo, contenido difamatorio o fraudulento). Al hacerlo, tienen la opción de ir por dos caminos: El primero es hacer aplicar la regulación gubernamental. En el segundo, basado en la autorregulación, los intermediarios mismos pueden decidir qué contenido es adecuado. Este camino presenta el riesgo de privatizar el control del contenido, ya que los intermediarios tomarían las responsabilidades de los gobiernos, pero tiene la ventaja de adoptar enfoques flexibles y de seguir el rápido ritmo de los avances tecnológicos. Esto es especialmente importante en el campo de la protección de los niños en línea.

Cada vez con mayor frecuencia, los tribunales de justicia imponen reglas a los intermediarios. En 2013, el TEDH ratificó una sentencia del tribunal de Estonia que declaró que el portal de noticias Delfi era responsable de los comentarios ofensivos publicados en su sitio web.[64] En junio de 2015, la Gran Sala del TEDH confirmó la sentencia de 2013: la decisión del tribunal de Estonia estaba fundada y era proporcionada, ya que los comentarios eran extremos y habían sido publicados como reacción a un artículo publicado por Delfi sobre su portal de noticias gestionado por profesionales y dirigido sobre una base comercial.[65] (La sentencia, sin embargo, no abarca otros espacios en línea en los que se pueden diseminar comentarios de terceros, como un foro de debate de Internet, un anuncio electrónico, o una plataforma social).

El rol de los intermediarios en las políticas contra el correo no deseado

Comúnmente, los PSI son tomados como las instituciones más involucradas en las iniciativas contra el correo no deseado. Los PSI por lo general tienen sus propias iniciativas para reducir el correo no deseado, ya sea mediante el filtrado técnico o la introducción de políticas anti-correo no deseado. Un informe de la UIT de 2006 sugiere que los PSI deberían ser

responsables del correo no deseado, y propuso un código de conducta en contra del correo no deseado, con dos disposiciones principales:

- Los PSI deben prohibir que sus usuarios envíen correos no deseados.
- Los PSI no deben relacionarse con PSI que no aceptan un código de conducta similar.[66]

El problema del correo no deseado dejó expuestas las nuevas dificultades de los PSI. Por ejemplo, el filtrado anti-correo no deseado de Verizon terminó en un caso judicial, ya que también bloqueaba mensajes legítimos, causando inconvenientes para los usuarios que no recibían sus correos electrónicos legítimos.[67] Ciertamente, los enfoques de auto y corregulación tomados por los PSI, junto con la cooperación internacional y el uso de filtros sofisticados, han minimizado la relevancia política del correo no deseado.

www.igbook.info/intermediaries

NOTAS FINALES

[1] Algunos de los primeros argumentos para el enfoque de derecho real fueron proporcionados por el juez Frank Easterbrook, quien, según se dice, señaló: «Váyanse a casa; el ciberderecho no existe». En el artículo *Cyberspace and the Law of the Horse*, indica que, si bien los caballos eran muy importantes, nunca hubo una Ley del Caballo. El juez Easterbrook argumenta que hay una necesidad de concentrarse en los instrumentos jurídicos básicos, como los contratos, las responsabilidades, etc, Disponible en http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2147&context=journal_articles [accedido el 24 de octubre de 2016]. El argumento de Easterbrook provocó muchas reacciones, incluida una de Lawrence Lessig en *The Law of the Horse: What Cyberlaw Might Teach*. Disponible en https://cyber.harvard.edu/works/lessig/LNC_Q_D2.PDF [accedido el 24 de octubre de 2016]. Para obtener más información sobre el debate entre los enfoques de derecho real y ciberderecho, consulte el blog The Oxford Comma: Shaping Internet Governance: Tensions Between 'Real' and 'Cyber' Laws. Disponible en http://wizardsqu1rrel.blogspot.com/2014/01/shaping-Internet-governance-tensions.html [accedido el 24 de octubre de 2016].

[2] Naciones Unidas (2013) Informe del Grupo de Expertos Gubernamentales de la ONU en el Campo de la información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. Disponible en http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf [accedido el 29 de octubre de 2016].

[3] Asamblea General de las Naciones Unidas (2015) Resolución A/70/125. Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información. Disponible en http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf [accedido el 27 de octubre de 2016].

[4] Asamblea General de las Naciones Unidas (2014) Resolución A/69/166. El derecho a la privacidad en la era digital. Disponible en http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166 [accedido el 29 de octubre de 2016]. Asamblea General de las Naciones Unidas (2012) Resolución A/HRC/20/L.13. Promoción, protección y disfrute de los derechos humanos en Internet. Disponible en http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280 [accedido el 29 de octubre de 2016].

[5] NTIA (1988) Statement of Policy on the Management of Internet Names and Addresses. Disponible en http://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-Internet-names-and-addresses [accedido el 24 de octubre de 2016].

[6] Por ejemplo, consideraron que el alcance del RTI se había extendido al incluir los PSI en una nueva disposición según la cual el reglamento sería aplicable a «aquellos organismos operacionales, autorizados o reconocidos por los Estados Miembros, para establecer, operar y participar en los servicios de telecomunicaciones internacionales al público». La controversia también rodeó la introducción de disposiciones concernientes a la seguridad de la red y las comunicaciones electrónicas no solicitadas. Debido a que se asocian con el concepto general de ciberseguridad (incluso en relación con el correo no deseado en el contexto de los correos electrónicos), se dice que es difícil interpretar que estas disposiciones son aplicables solamente para las telecomunicaciones tradicionales (y no para Internet). Además de las diferentes interpretaciones, algunos consideran que la definición de telecomunicación (que no cambió en relación con la versión de 1988) también cubre las comunicaciones realizadas a través de Internet: «Toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos, o informaciones de cualquier naturaleza por hilo, radioelectricidad, medio óptico u otros sistemas electromagnéticos».

[7] Ago R (1956) Science juridique et droit international. Receuil des Cours Academie de Droit International (RCADI), 1956-II, 855–954, La Haya

[8] Convenio de Viena sobre el Derecho de los Tratados. Disponible en https://www.ilsa.org/jessup/jessup11/basicmats/VCLT.pdf [accedido el 28 de octubre de 2016].

[9] Brownlie I (1999) *Principles of Public International Law,* 5th Ed. Oxford: Oxford University Press, p. 513.

[10] Salis RP (2001) A Summary of the American Bar Association's (ABA) Jurisdiction in Cyberspace Project: Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet. Disponible en http://www.jstor.org/stable/40687955 [accedido el 28 de octubre de 2016].

[11] Entre los recursos más importantes en este campo, se encuentra *Princeton Principles on Universal Jurisdiction* (2001). Disponible en http://hrlibrary.umn.edu/instree/princeton.html [accedido el 28 de octubre de 2016].

[12] Malanczuk P (1997) *Akehurst's Modern Introduction to International Law.* Londres: Routledge, p. 113.

[13] EDRI-gram (2006) French anti-hate groups win case against Yahoo! Disponible en http://edri.gn.apc.org/edrigram/number4.1/yahoocase [accedido el 24 de octubre de 2016].

[14] TJUE (2011) Sentencia del Tribunal de justicia en los asuntos acumulados C-509/09 y C-161/10: eDate Advertising GmbH vs X, y Olivier Martinez, Robert Martinez vs MGN Limited. Disponible en http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-509/09&td=ALL [accedido el 29 de octubre de 2016].

[15] TJUE (2013) Sentencia del Tribunal en el caso C-170/12: Peter Pinckney vs KDG Mediatech AG. Disponible en http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-170/12&td=ALL [accedido el 29 de octubre de 2016].

[16] Para obtener una revisión de los casos que involucran una jurisdicción extraterritorial relacionados con el contenido en Internet, consulte: Timofeeva YA (2005) Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis. *Connecticut Journal of International Law, 20*, 199. Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=637961 [accedido el 24 de octubre de 2016].

[17] Un caso relativamente similar fue el del Tribunal Federal de Justicia de Alemania contra Frefrick Toben, exciudadano alemán de nacionalidad australiana, quien había publicado en un sitio web basado en Australia material que cuestionaba la existencia del holocausto. Disponible en http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html [accedido el 24 de octubre de 2016].

[18] Commission Nationale de l'Informatique et des Libertés (2015) Derecho a la supresión: Apelación informal de Google denegada. Disponible en https://www.cnil.fr/fr/node/15814 [accedido el 11 de octubre de 2016].

[19] TJUE (2015) Sentencia del Tribunal en el caso C-362/14: Maximillian Schrems vs el Comisionado de Protección de Datos. Disponible en http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2015 [accedido el 21 de octubre de 2016].

[20] Tribunal de Apelaciones del Segundo Circuito de EE. UU. (2016) Sentencia sobre la orden de registro de una dirección de correo electrónico determinada, controlada y mantenida por Microsoft Corporation: Microsoft Corporation vs EE. UU. Disponible http://www.ediscoverylaw.com/wp-content/uploads/2016/07/In-re-Matter-of-a-Warrant.pdf [accedido el 24 de octubre de 2016].

[21] La orden judicial, en francés, está disponible en http://www.cottineau.net/wp-content/uploads/2016/02/facebook-jugement-cour-appel-paris-12-fevrier-2016.pdf [accedido el 12 de octubre de 2016].

[22] Yaron O (2016) Israeli judge approves $400 million class action against Facebook for violating privacy. *Haaretz*, 17 de junio. Disponible en http://www.haaretz.com/israel-news/business/1.725512 [accedido el 12 de octubre de 2016].

[23] Algunos ejemplos de asuntos controvertidos son: el contenido racista, la pornografía, las apuestas en línea, la publicidad del tabaco, y la venta de drogas.

[24] UNCITRAL (1958) La Convención de Nueva York. Disponible en http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html [accedido el 24 de octubre de 2016].

[25] CNUDMI (1985) Ley Modelo sobre Conciliación Comercial Internacional. Disponible en http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/1985Model_arbitration.html [accedido el 24 de octubre de 2016].

[26] OMPI (sin fecha) Resolución de Disputas de Nombres de Dominio. Disponible en http://www.wipo.int/amc/en/domains/ [accedido el 25 de octubre de 2016].

[27] Comisión Europea (2016) Resolución de litigios de los consumidores en línea. Disponible en http://ec.europa.eu/consumers/solving_consumer_disputes/docs/adr-odr.factsheet_web.pdf [accedido el 25 de octubre de 2016].

[28] Google (2016) Informe de Transparencia. Solicitudes europeas de privacidad relacionadas con la eliminación de resultados. Disponible en https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en [accedido el 29 de octubre de 2016].

[29] OMPI (sin fecha) Tratado de la OMPI sobre Derecho de Autor. Disponible en http://www.wipo.int/treaties/en/ip/wct/ [accedido el 1 de noviembre de 2016].

[30] Oficina del Representante de los Estados Unidos para Asuntos Comerciales (sin fecha) Acuerdo Transpacífico. Disponible en https://ustr.gov/tpp/ [accedido el 1 de noviembre de 2016].

[31] Congreso de EE. UU. (1998) Ley de Derechos de Autor de la Era Digital. Disponible en http://www.copyright.gov/legislation/hr2281.pdf [accedido el 1 de noviembre de 2016].

[32] Congreso de EE. UU. (2011) Ley de cese de la piratería en línea (SOPA). Disponible en https://www.congress.gov/bill/112th-congress/house-bill/3261 [accedido el 24 de octubre de 2016].

[33] Congreso de EE. UU. (2011) Ley Protect IP. Disponible en https://www.congress.gov/bill/112th-congress/senate-bill/968 [accedido el 24 de octubre de 2016].

[34] Acuerdo Comercial Anti-Falsificación (2011) Disponible en http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147937.pdf [accedido el 24 de octubre de 2016].

[35] La Quadrature du Net, un grupo de defensa de derechos humanos, siguió de cerca los desarrollos sobre la ley Hadopi y elaboró un expediente completo sobre la ley ACTA. Disponible en http://www.laquadrature.net/en/ACTA [accedido el 25 de octubre de 2016]. Sobre las protestas en contra de los proyectos de EE. UU., consulte: Vijayan J (2012) Protests against SOPA, PIPA go viral. *Computerworld*, 18 de enero. Disponible en http://www.computerworld.com.au/article/412655/protests_against_sopa_pipa_go_viral/ [accedido el 25 de octubre de 2016].

[36] Sorkin AR (2003) Software bullet is sought to kill musical piracy. *New York Times,* 4 de mayo. Disponible en http://www.nytimes.com/2003/05/04/business/04MUSI.html [accedido el 25 de octubre de 2016].

[37] Oficina de Patentes y Marcas de Estados Unidos (sin fecha) Propiedad Intelectual y la Infraestructura Nacional. Disponible en https://www.uspto.gov/web/offices/com/doc/ipnii/ [accedido el 25 de octubre de 2016].

[38] Para obtener una explicación sobre el concepto del uso legítimo y algunos ejemplos, consulte: The UK Copyright Service (sin fecha) Copyright Law fact sheet P-09: Understanding Fair Use. Disponible en http://www.copyrightservice.co.uk/copyright/p09_fair_use [accedido el 25 de octubre de 2016].

[39] NTIA (1998) Statement of Policy on the Management of Internet Names and Addresses. Disponible en https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses [accedido el 1 de noviembre de 2016].

[40] Para obtener un estudio más completo sobre los principales asuntos con respecto a la UDRP, consulte: OMPI (2011) WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Second Edition (WIPO Overview 2.0) Disponible en http://www.wipo.int/amc/en/domains/search/overview2.0/ [accedido el 25 de octubre de 2016].

[41] Para obtener más detalles sobre el caso .amazon, consulte: Murphy K (2016) Amazon files appeal on rejected .amazon domain. *The Register,* 3 de marzo de 2016. Disponible en http://domainincite.com/20105-amazon-files-appeal-on-rejected-amazon-domain [accedido el 25 de octubre de 2016]. Para obtener más detalles sobre el IRP iniciado por Amazon, consulte: ICANN (sin fecha) Amazon EU S.à.r.l. vs ICANN (.AMAZON). Disponible en https://www.icann.org/resources/pages/irp-amazon-v-icann-2016-03-04-en [accedido el 25 de octubre de 2016].

[42] Decker S and Robertson D (2016) VirnetX Wins $302.4 Million Trial Against Apple in Texas. Bloomberg, 30 de septiembre. Disponible en https://www.bloomberg.com/news/articles/2016-10-01/virnetx-wins-302-4-million-trial-against-apple-in-texas [accedido el 25 de octubre de 2016].

[43] Loney M (2002) Hyperlink patent case fails to click. *CNET*, 23 de agosto. Disponible en https://www.cnet.com/news/hyperlink-patent-case-fails-to-click/ [accedido el 25 de octubre de 2016].

[44] Oficina Europea de Patentes (sin fecha) ¿Patentar software? Derecho y práctica europeos. Disponible en https://www.epo.org/news-issues/issues/software.html [accedido el 25 de octubre de 2016].

[45] Somerville H (2015) Former Uber driver was an employee, rules California department. *Reuters*, 9 de septiembre. Disponible en http://www.reuters.com/article/uber-tech-california-ruling-idUSL1N11F1KT20150910 [accedido el 29 de octubre de 2016].

[46] Departamento de Trabajo e Industrias del Estado de Oregón (2016) Advisory opinion of the Commissioner of the Bureau of Labor and Industries regarding the employment status of Uber drivers. Disponible en http://media.oregonlive.com/commuting/other/101415%20Advisory%20Opinion%20on%20the%20Employment%20Status%20of%20Uber%20Drivers.pdf [accedido el 29 de octubre de 2016].

[47] Ampel C (2015) Florida: Uber drivers are contractors, not employees. *Daily Business Review*, 4 de diciembre. Disponible en http://www.dailybusinessreview.com/id=1202743938454/Florida-Uber-Drivers-Are-Contractors-Not-Employees?slreturn=20160929162026 [accedido el 29 de octubre de 2016].

[48] TEDH (2007) Sentencia del Tribunal sobre el Caso Copland vs el Reino Unido (aplicación nº 62617/00). http://hudoc.echr.coe.int/eng?i=001-79996 [accedido el 29 de octubre de 2016].

[49] TEDH (2016) Sentencia del Tribunal sobre el Caso Bărbulescu vs Rumania (Aplicación nº 61496/08). Disponible en http://hudoc.echr.coe.int/eng?i=001-159906 [accedido el 29 de octubre de 2016].

[50] Consulte los siguientes artículos a modo de ejemplo: Holding R *(2011)* Can You Be Fired for Bad-Mouthing Your Boss on Facebook? *Time U.S.*, 4 de marzo. Disponible en http://www.time.com/time/nation/article/0,8599,2055927,00.html [accedido el 25 de octubre de 2016]. Broughton A *et al.* (2009) Workplaces and Social Networking. The Implications for Employment Relations. Disponible en http://www.acas.org.uk/media/pdf/d/6/1111_Workplaces_and_Social_Networking.pdf [accedido el 25 de octubre de 2016].

[51] CMSI (2003) Declaración de Principios. Construir la Sociedad de la Información: un desafío global para el nuevo milenio. Disponible en http://www.itu.int/net/wsis/docs/geneva/official/dop.html [accedido el 29 de octubre de 2016].

[52] La definición práctica que la OCDE da para los intermediarios intenta identificar las varias categorías de proveedores de servicios que entran bajo el concepto de «intermediarios»: «Los intermediarios de Internet reúnen o facilitan las transacciones entre terceros en Internet. Dan acceso, alojan, transmiten, e indexan contenido, productos y servicios provenientes de terceros en Internet o brindan servicios basados en Internet a terceros». En: OCDE (2011) El papel de los intermediarios de Internet en su avance hacia el cumplimiento de los objetivos de políticas públicas relacionadas con las TIC. Disponible en http://www.oecd.org/sti/ieconomy/theroleofinternetintermediariesinadvancingpublicpolicyobjectives.htm [accedido el 29 de octubre de 2016].

[53] OCDE (2011) Recomendación del Consejo de la OCDE sobre los Principios para la Elaboración de Políticas de Internet. Disponible en http://www.oecd.org/Internet/ieconomy/49258588.pdf [accedido el 10 de octubre de 2016].

[54] MacKinnon R *et al.* (2014) Fostering Freedom Online. The Role of Internet Intermediaries. UNESCO/Internet Society. Disponible en http://unesdoc.unesco.org/images/0023/002311/231162e.pdf [accedido el 10 de octubre de 2016].

[55] Unión Europea (2000) Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).Disponible en http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32000L0031 [accedido el 25 de octubre de 2016]. Unión Europea (2001) Directiva

2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información. Disponible en http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1477400249287&uri=CELEX:32001L0029 [accedido el 25 de octubre de 2016].

[56] El procedimiento de «detección y eliminación» hace referencia a la obligación de los proveedores de servicios de eliminar contenido de los sitios web bajo su administración cuando reciban una notificación o denuncia que tenga que ver con la legalidad de ese contenido en particular.

[57] Ante el miedo de enfrentar sanciones legales, algunos PSI prefieren restringir el acceso a un contenido determinado incluso cuando no se ha cometido ninguna violación. Para obtener más detalles, consulte los siguientes estudios: Para Europa (los Países Bajos): Nas S (2004) *The Multatuli Project ISP Notice & Take Down,* Bits of Freedom. Disponible en https://www-old.bof.nl/docs/researchpaperSANE.pdf [accedido el 28 de octubre de 2016]. Para EE. UU.: Urban J and Quilter L (2006) *Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act.* Disponible en http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1500&context=facpubs [accedido el 28 de octubre de 2016].

[58] «La Corte de Apelaciones de La Haya falló en contra de la Iglesia de Cienciología en su demanda de violación del derecho de autor contra una escritora holandesa y su PSI, XS4ALL. La escritora, exciencióloga practicante, publicó en un sitio web partes de los documentos confidenciales de la iglesia, y en consecuencia, la iglesia la demandó bajo la Ley sobre el Derecho de Autor de Holanda de 1992. En 1999, la Corte del Distrito falló a favor de los acusados, señalando inquietudes sobre la libertad de expresión. Sin embargo, esa corte también sentenció que los PSI debían hacerse responsables de los materiales publicados que pueden violar los derechos de autor existentes. La Corte de Apelaciones ratificó la primera sentencia, pero revocó la segunda, y sostuvo que los PSI no eran responsables de los materiales publicados». Para obtener más información, consulte: Gelman L (2003) Church of Scientology Loses Copyright Infringement Case in Dutch Court. Disponible en http://cyberlaw.stanford.edu/packets001638.shtml [accedido el 25 de octubre de 2016].

[59] Para obtener más información acerca de este caso, consulte: Electronic Privacy Information Center (2004) RIAA *vs* Verizon. Disponible en https://epic.org/privacy/copyright/verizon/ [accedido el 25 de octubre de 2016].

[60] La Corte Suprema de Canadá rechazó el argumento de la Sociedad de Compositores, Autores y Editores de la Música de Canadá sobre que los PSI canadienses debían pagar derechos de autor porque algunos de sus clientes descargan obras protegidas por este derecho (SOCAN vs CAIP). Para obtener más información, visite http://www.canlii.org/en/ca/scc/doc/2004/2004scc45/2004scc45.html [accedido el 25 de octubre de 2016].

[61] «SABAM (la sociedad colectiva belga – *Société belge des auteurs, compositeurs et* éditeurs) pedía que el PSI Scarlet instale un sistema de filtrado generalizado para todas las comunicaciones electrónicas entrantes y salientes a través de sus servicios y que bloquee las comunicaciones potencialmente ilícitas. En la Primera Instancia, aunque rechazó la responsabilidad del PSI, el Tribunal de Bruselas concluyó que el reclamo de SABAM era legítimo y que debía implementarse el sistema de filtrado. Scarlet apeló y el caso se delegó al Tribunal de Justicia de la Unión Europea. En su decisión el Tribunal de Justicia sentenció que un sistema de filtrado y bloqueo para todos sus clientes por un lapso indeterminado, *in abstracto* y como medida de prevención, viola derechos fundamentes, particularmente el derecho a la privacidad, la libertad a la comunicación y a la información. Adicionalmente, viola la libertad del PSI a desarrollar sus actividades comerciales». Para obtener más información, consulte: TJUE (2011) Sentencia del Tribunal en el caso C-70/10: Scarlet Extended SA vs Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Disponible en http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-70/10&td=ALL [accedido el 25 de octubre de 2016].

[62] TJUE (2016) Sentencia del Tribunal en el caso C-160/15: GS Media BV vs Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruida Dekker. Disponible en http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-160/15&td=ALL [accedido el 25 de octubre de 2016].

[63] En 2013, se derogó una parte de la ley Hadopi, ya que la sanción de suspender el acceso a Internet por parte del infractor se consideró desproporcionada.

[64] TEDH (2013) Sentencia del Tribunal (Sección Primera) en el caso Delfi AS vs Estonia (Aplicación nº 64569/09). Disponible en http://hudoc.echr.coe.int/eng?i=001-126635 [accedido el 29 de octubre de 2016].

[65] TEDH (2015) Sentencia del Tribunal (Gran Sala) en el caso Delfi AS vs Estonia (Aplicación nº 64569/09). Disponible en http://hudoc.echr.coe.int/eng?i=001-155105 [accedido el 29 de octubre de 2016].

[66] Palfrey J (2006) Stemming the International Tide of Spam. En: UIT (2006) Tendencias en las reformas de telecomunicaciones. Disponible en http://www.itu.int/ITU-D/treg/publications/Chap%207_Trends_2006_E.pdf [accedido el 29 de octubre de 2016].

[67] Shannon V (2006) The end user: Junk payout in spam case – Technology – International Herald Tribune. *The New York Times*, 26 de abril. Disponible en http://www.nytimes.com/2006/04/12/technology/12iht-PTEND13.1523942.html [accedido el 28 de octubre de 2016].

Sección 5

LA CANASTA ECONÓMICA

La canasta económica

Sabemos cómo enrutar paquetes
Lo que no sabemos es cómo enrutar dólares.

David Clark – Principal Arquitecto de Protocolo de Internet

Esta cita de David Clark refleja el espíritu de la primera comunidad de Internet, en la que el proyecto de una Internet sin fines de lucro se apoyaba en, principalmente, becas de investigación de EE. UU. Sin embargo, en la década de 1990 y 2000, comenzaron a surgir en Silicon Valley nuevos modelos de negocio para «enrutar dólares», centrados principalmente en los ingresos a partir de la publicidad.

Los asuntos económicos en la gobernanza de Internet están relacionados, principalmente, con esta evolución de la Internet como un proyecto sin fines de lucro hacia una Internet que sería uno de los principales servicios y motores para el crecimiento económico de la sociedad moderna. El fluir de las ideas y la creatividad que ha facilitado la Internet desde su etapa más temprana se ha complementado con la competencia del fluir del dinero, y, cada vez más, se encuentra en competencia con él. Una mayor inversión de dinero dio lugar a negocios e intereses políticos más tangibles. El enfoque creativo «el cielo es el límite» de la comunidad temprana de Internet comenzó a reemplazarse por la lógica del «resultado final» de la comunidad empresarial. La interacción entre la gran creatividad y el robusto apoyo económico impulsaron una real revolución económica geográficamente centrada en la zona de San Francisco en California.

Las políticas digitales afectan y se ven afectadas por los desarrollos económicos y el flujo de dinero.[1] Una política digital habilitante es esencial para el crecimiento económico. Una de las razones del rápido crecimiento económico en Silicon Valley, por ejemplo, fue el sistema regulatorio financiero; este sistema ha protegido la propiedad intelectual de las compañías de Internet y ha incentivado las inversiones, además de muchas otras cosas. La importancia de los suplementos «análogos» (un entorno político habilitante) para la economía digital estuvo bajo la lupa del Banco Mundial en su Informe de Desarrollo Mundial 2016: Dividendos Digitales.[2]

Las políticas digitales también se ven afectadas por las compañías de Internet. Estas desarrollaron poderosas máquinas de presión, que están particularmente activas en los centros de políticas digitales más importantes, como Washington D.C., Bruselas, y Ginebra.

Nuestro análisis de temas relacionados con la economía de la Internet se enfoca en cuatro dominios principales en los que ocurren las transacciones empresariales monetarias y no monetarias.

- Comercio electrónico: actividades comerciales tradicionales llevadas a cabo por medio de Internet.

- Economía de DATOS de Internet: el nuevo modelo de negocio basado en la publicidad.
- Economía de ACCESO a Internet: la industria de las telecomunicaciones en la era de Internet.
- Banca electrónica, dinero electrónico, y monedas virtuales.

Además, examinamos otros dos temas políticos de relevancia económica: la protección del consumidor y las cargas fiscales.

Comercio electrónico

El comercio electrónico ha sido uno de los más fuertes motores que impulsaron el crecimiento de Internet durante los últimos 15 años. La importancia del comercio electrónico quedó ilustrada en el título del documento que inició la reforma de la gobernanza de Internet y abrió camino para la creación de ICANN: el Marco para el Comercio Electrónico Global[3] de 1997, que estipula que «el sector privado debe liderar» el proceso de la gobernanza de Internet y que la función principal de esta gobernanza sería «propiciar que el comercio tenga un entorno jurídico simple, predecible, minimalista, y coherente».

Hoy en día, el impacto del comercio electrónico en las personas y empresas es de amplio alcance. El comercio electrónico proporcionó muchas ventajas para los consumidores, como la comodidad de las compras en línea, la flexibilidad de la facilidad de acceso a distintos mercados, y las operaciones bancarias en línea y de pago electrónico, que ahorran mucho tiempo. Desde el punto de vista empresarial, el comercio electrónico influenció la gestión de la cadena de abastecimiento, y permitió que las compañías lleguen a sus clientes más fácilmente, mediante la publicidad y el marketing en línea y otros caminos. Sin embargo, las empresas se enfrentan a una competencia más feroz y a otras complejidades cuando ofrecen un mercado en línea.

Definición

La elección de una definición para el comercio electrónico conlleva muchas inferencias prácticas y legales. Se aplican reglas específicas cuando una transacción en particular se considera comercio electrónico, como las reglas de cargas fiscales y aduanas.

Para el gobierno de EE. UU., el elemento clave que distingue el comercio tradicional del electrónico es el compromiso en línea de la venta de bienes o servicios. Esto implica que cualquier transacción comercial celebrada en línea debería tomarse como una transacción de comercio electrónico, incluso si la consecución de esa transacción incluye una entrega física. Por ejemplo, adquirir un libro a través de Amazon.com se considera una transacción de comercio electrónico, aunque el libro generalmente llega al cliente mediante el correo tradicional. La OMC define al comercio electrónico de una manera más precisa: «la producción, distribución, comercialización, venta, o entrega de bienes y servicios por medios electrónicos».[4] El enfoque de la UE sobre el comercio electrónico aborda los «servicios de la sociedad de la información» que cubren «cualquier servicio prestado normalmente a título oneroso, a distancia, mediante un equipo electrónico para el tratamiento (incluida la compresión digital) y el almacenamiento de datos, y a petición individual de un receptor de un servicio».[5]

El comercio electrónico se presenta de muchas formas:

- Comercio a consumidor (B2C) – es el tipo de comercio electrónico más conocido (por ejemplo, Amazon.com).
- Comercio a comercio (B2B) – es el más intenso económicamente ya que representa más del doble del tamaño del mercado B2C.[6]
- Comercio a gobierno (B2G) – es altamente importante en el área de políticas de contratación pública.
- Consumidor a consumidor (C2C) – por ejemplo, las subastas de eBay.

Muchos países están elaborando marcos normativos para el comercio electrónico. Se promulgaron leyes en varios campos de relevancia, como las firmas digitales, la resolución de conflictos en línea, la ciberdelincuencia, la protección del consumidor, y las cargas fiscales de los servicios electrónicos. A nivel internacional, un creciente número de iniciativas y regímenes están relacionados con el comercio electrónico.

La OMC y el comercio electrónico

Como actor político clave en el comercio mundial moderno, la OMC estableció un sistema de acuerdos que regulan el comercio internacional. Los tratados más importantes son el Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT, por sus siglas en inglés)[7] que trata sobre el comercio de bienes, el Acuerdo General sobre el Comercio de Servicios (GATS, por sus siglas en inglés)[8], y TRIPS (Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio).[9] Dentro de este marco, la OMC regula los temas más relevantes del comercio electrónico, incluidos la liberalización de las telecomunicaciones, los DPI, y algunos aspectos del desarrollo de las TIC. El comercio electrónico se ve representado en las siguientes actividades e iniciativas de la OMC:

- Una moratoria temporaria sobre los derechos de aduana sobre las transmisiones electrónicas, introducida en 1998, dejó sin aranceles aduaneros a todas las transmisiones electrónicas entre los estados miembros de la OMC.[10]
- El Programa de Trabajo sobre el Comercio Electrónico de la OMC, establecido en 1998, describe las responsabilidades de los órganos de la OMC en áreas relacionadas con el comercio electrónico.[11]
- Un mecanismo de resolución de conflictos que aborda, entre otras cosas, los casos relativos a las transacciones electrónicas. (Un ejemplo es el caso de las apuestas en línea de EE. UU./Antigua, en el que el comercio electrónico fue especialmente relevante[12]).

Si bien la diplomacia de la OMC ha puesto en segundo plano al comercio electrónico, surgieron muchas iniciativas y se identificaron varios temas clave, incluidos los que se explican a continuación:

¿Las transacciones de comercio electrónico entran dentro de la categoría de servicios (regulados por el GATS) o bienes (regulados por el GATT)?

Muchas transacciones de comercio electrónico son de carácter dual. En las primeras etapas digitales, el principal dilema residía entre categorizar la música como un bien o como

un servicio, dependiendo de su soporte: en CD (tangible) o a través de Internet (intangible). Básicamente, la misma canción podía tener un estatus comercial diferente (y estar sujeta a diferentes costos aduaneros e impositivos) dependiendo de su soporte de entrega. La cuestión la categorización emerge también en el contexto de transacciones combinadas que involucran elementos intangibles (celebración del contrato en línea, distribución de *software*) y elementos tangibles (entrega física de una impresora u otros dispositivos digitales). Este tipo de transacción será de una mayor importancia con los avances en el campo de la IoT. El problema de la categorización tiene consecuencias considerables, debido a los diversos mecanismos normativos para los bienes y servicios.

¿Cuál debería ser la conexión entre el TRIPS y la protección de los DPI en Internet?

Debido a que el acuerdo TRIPS de la OMC brinda una aplicación de los mecanismos mucho más estricta para los DPI que para los tratados de la OMPI, los países desarrollados han estado intentando extender la cobertura del TRIPS hacia el comercio electrónico y a la Internet mediante el uso de dos enfoques: El primero, que cita el principio de «neutralidad tecnológica», afirma que el TRIPS, como otras reglas de la OMC, debería extenderse a cualquier medio de telecomunicación, incluida Internet. En el segundo, algunos países desarrollados solicitaron una integración más estrecha de los «tratados digitales» de la OMPI en el sistema del TRIPS. Ambos temas se mantienen abiertos y es posible que sean cada vez más importantes en el futuro de las negociaciones de la OMC. La falta de acuerdos mundiales sobre comercio electrónico se compensará, en parte, gracias a algunas iniciativas específicas (por ejemplo, con respecto a los contratos y las firmas) y varios acuerdos regionales, principalmente en la UE y la región Asia-Pacífico.

El futuro rol de la OMC en el comercio electrónico

Debates actuales discuten si la OMC debería cumplir un rol más importante en el comercio electrónico. Durante el Foro Público de la OMC en septiembre de 2016, se aseveró que la organización podría incorporar de una manera más decidida en su agenda al comercio electrónico y la economía digital en general.[13] Sin embargo, los estados miembros no parecen ponerse de acuerdo en este asunto. Algunos están dispuestos a concentrarse más en el comercio electrónico y considerar marcos multilaterales en ese campo, mientras que otros son de la opinión de que existen otras prioridades en la OMC en las que debería enfocarse (como el acceso a la infraestructura y las habilidades digitales) antes de empezar a debatir sobre los marcos normativos.[14]

El comercio electrónico y otros asuntos de políticas digitales

Hacer una clara distinción entre el comercio electrónico y otros temas de gobernanza de Internet es cada vez más desafiante. Por ejemplo, la dimensión comercial de la economía de datos se ve inevitablemente afectada por las regulaciones de los derechos humanos sobre la privacidad y la libertad a la información (asuntos que se abordan, por ejemplo, dentro del CDH de la ONU), los estándares para la transacción de datos (desarrollados por ISO, la IETF, y la UIT), la ciberseguridad – donde los datos cumplen un rol cada vez más importante en la lucha contra el terrorismo y el crimen (GGE de la ONU, UNODC). Si bien la OMC no puede (y no debería) lidiar completamente con la complejidad de las políticas digitales más allá del comercio, la organización debe desarrollar mecanismos para sincronizar su trabajo sobre el comercio electrónico con el trabajo de otros organismos internacionales, que inevitablemente provocarán un impacto en las regulaciones de la OMC sobre el comercio electrónico.

Otras iniciativas sobre el comercio electrónico mundial

Existen muchas organizaciones internacionales que se ocupan de los temas relacionados con el comercio electrónico. La CNUDMI (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) ha llevado a cabo una importante labor en esta área. En 1992, esta comisión formó un Grupo de Trabajo sobre el Intercambio Electrónico de Datos (que luego se convirtió en el Grupo de Trabajo sobre el Comercio Electrónico), cuya labor llevo, entre otras cosas, a la adopción de la Ley Modelo de la CNUDMI sobre Comercio Electrónico[15] y Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales.[16] La Ley Modelo resultó ser una de las iniciativas más exitosas y de más amplio respaldo internacional en este campo; se enfoca en mecanismos para la integración del comercio electrónico y el derecho comercial tradicional (por ejemplo, reconoce la validez de los documentos electrónicos). La Ley Modelo se utilizó como base para la regulación del comercio electrónico en muchos países.

Otra iniciativa en el campo del comercio electrónico es la iniciativa Electronic Business XML (ebXML), lanzada por el Centro de las Naciones Unidas para la Facilitación del Comercio y el Comercio Electrónico (CEFACT, en inglés) y la Organización para el Avance de Estándares de Información Estructurada (OASIS, por sus siglas en inglés). El objetivo de la iniciativa es desarrollar las especificaciones técnicas abiertas y relevantes en apoyo a los intercambios comerciales electrónicos nacionales e internacionales.[17] Aunque se están desarrollando nuevas especificaciones, todavía se emplea la serie anterior – Intercambio Electrónico de Datos (EDI, por sus siglas en inglés). Queda por ver si se ajustan – y de ser así, cómo – para poder estar a la altura de las nuevas tendencias y los nuevos desarrollos tecnológicos.

La Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD, por sus siglas en inglés) tiene un rol particularmente activo en la investigación y la construcción de capacidades, y se centra en la relevancia del desarrollo del comercio electrónico. Cada año, monitorea la evolución de la economía de la información y publica el Informe sobre la Economía de la Información, que evalúa el rol de las nuevas tecnologías en el comercio y el desarrollo.[18] En 2016, la UNCTAD lanzó la Iniciativa Comercio Electrónico para Todos, un proyecto de múltiples partes interesadas destinado a mejorar la habilidad de los países en vías de desarrollo para usar y sacar provecho del comercio electrónico.[19]

Las actividades de la OCDE abordan varios aspectos del comercio electrónico, como la protección del consumidor y las firmas digitales. Su participación en el comercio electrónico comenzó con el Plan de Acción para el Comercio Electrónico de 1998, estructurado sobre la base de cuatro objetivos principales: generar confianza para los usuarios y consumidores, establecer reglas básicas para el mercado digital, mejorar la infraestructura de la información para el comercio electrónico, y maximizar sus beneficios.[20] Las recomendaciones y directrices de la OCDE actúan en favor de estos objetivos desde entonces.

El G20 también le ha prestado una especial atención a los asuntos relacionados con el comercio electrónico en los últimos años. Durante la Cumbre de Líderes del G20 en Hangzhou, China (septiembre de 2016), los miembros del G20 destacaron que el comercio electrónico era una de sus prioridades.[21] Los líderes también tomaron nota de una iniciativa para crear una Plataforma de Comercio Electrónico Mundial, principalmente para asistir a que las pequeñas y medianas empresas (PyMEs) ingresen al mercado de comercio electrónico mundial.

En el sector comercial, una de las organizaciones internacionales más activas es la Cámara de Comercio Internacional (CCI), que elabora una amplia gama de recomendaciones y análisis en el campo del comercio electrónico.

Otra iniciativa que vale la pena traer a colación es el Pacto Global de la ONU. Aunque no está destinado específicamente a abordar temas relativos al comercio electrónico, la iniciativa se ocupa de crear conexiones más sólidas entre las empresas y los derechos humanos, y de apoyar a las compañías para que hagan negocios de una manera responsable, alineando sus estrategias y operaciones con los principios universales sobre derechos humanos. Gracias a que los aspectos concernientes a la protección de los derechos humanos en el entorno digital influencian cada vez más la manera en la que trabajan las compañías de Internet, se espera que esta iniciativa tenga un impacto significativo en la industria de Internet, incluida el área del comercio electrónico.

Iniciativas regionales

La UE desarrolló su primera estrategia de comercio electrónico en la cumbre denominada Dot Com Summit de los líderes de la UE en Lisboa (marzo de 2000). Aunque acogía un enfoque privado y centrado en el mercado con respecto al comercio electrónico, la UE también introdujo algunas medidas correctivas destinadas a proteger los intereses públicos y sociales (la promoción del acceso universal, una política de competencia que tenga en consideración el interés público, y la restricción en la distribución de contenido dañino). Más tarde, en 2015, se incorporó la Estrategia para el Mercado Único Digital. Se enfoca específicamente en el comercio electrónico, y cuenta con objetivos para facilitar un mejor acceso a los bienes y servicios digitales, y para fortalecer la economía digital como motor impulsor del crecimiento.

La UE también cuenta con una Directiva sobre el Comercio Electrónico (dedicada a brindar un marco jurídico uniforme y completo para el comercio electrónico para todos los estados miembros de la UE), así como también una serie de distintos documentos legales que abordan temas como el de las firmas electrónicas, la protección de datos, y las transacciones financieras electrónicas.

En la región Asia-Pacífico, el punto de concentración de cooperación para el comercio electrónico es la APEC. Uno de los primeros programas relacionados con el comercio electrónico de la APEC fue el Programa para la Acción en el Comercio Electrónico de APEC de 1998, que tenía la finalidad de consolidar y reforzar las varias iniciativas de APEC en esta área. Para implementar este plan, se estableció un Grupo de Dirección para hacer frente a varias cuestiones de comercio electrónico, como la protección del consumidor, la protección de datos, el correo no deseado, y la ciberseguridad. La iniciativa más prominente es el Plan de Acción Individual para el Comercio sin Papel[22] de APEC, cuyo fin es crear sistemas sin papel en el comercio transfronterizo.

Dentro de la ASEAN, se creó un Grupo de Trabajo para la Facilitación del Comercio mediante el Comercio Electrónico y las TIC, con el objetivo de contribuir al desarrollo de marcos legislativos y normativos que construyan la confianza de los consumidores. En este sentido, el grupo inició un Proyecto de Infraestructura Legal para el Comercio Electrónico, dedicado a formular directrices para una infraestructura jurídica aplicable al comercio electrónico, y a facilitar el desarrollo y crecimiento de comercio y negocio electrónico confiables tanto dentro de los países de la ASEAN, como entre ellos.

El Mercado Común de África Oriental y Austral (COMESA, por sus siglas en inglés) también está llevando a cabo actividades en el área del comercio electrónico. La Estrategia del COMESA explica el compromiso de la organización para promover de manera activa el comercio electrónico para mejorar la integración digital del mercado común. En 2010, el

Consejo del COMESA adoptó una Ley Modelo sobre las Transacciones Electrónicas, que contiene disposiciones sobre firmas electrónicas, comercio electrónico, protección del consumidor, comunicaciones comerciales no solicitadas, y resolución de conflictos en línea.[23]

Iniciativas plurilaterales

Las iniciativas plurilaterales reúnen a países de diferentes regiones interesados en los mismos asuntos. El enfoque plurilateral se usa cada vez más en el contexto de la OMC. En el último tiempo, se negociaron varios acuerdos transregionales, y es probable que causen un impacto significativo en las políticas digitales. Dos de los acuerdos más notables son el Acuerdo de Asociación Transpacífico (TPP, por sus siglas en inglés), firmado en febrero de 2016, y el Asociación Transatlántica para el Comercio y la Inversión (TTIP, por sus siglas en inglés), que todavía está en negociación desde octubre de 2016. Estos acuerdos comerciales afectarían no solo al comercio electrónico, sino también a la reglamentación sobre datos y la resolución de conflictos en Internet.

www.igbook.info/ecommerce

Economía de DATOS de Internet

El nuevo modelo de negocios (Figura 19) de la industria de Internet, desarrollado principalmente por compañías de Silicon Valley, comenzó a dejarse ver a finales de la década de 1990, y terminó de formarse en la década de 2010. El crecimiento de Internet en la década de 1990 no podía mantenerse mediante el financiamiento público, como en el pasado; este exigía un modelo de negocio más robusto. Los intentos de cobrar el acceso a los servicios y contenidos de Internet fue un fracaso. El nuevo modelo de negocios de Internet no cobra

Figura 19. Modelo de negocios de la industria de Internet

a los usuarios por el uso de los servicios que brinda Internet sino que genera sus ganancias a partir de publicidad sofisticada.

En el nuevo modelo de negocio, los datos del usuario son El principal recurso económico. Al buscar información e interactuar en Internet, los usuarios revelan cantidades de datos relevantes, incluso datos personales y la información que ellos mismos generan su «huella electrónica». Las compañías de Internet recopilan y analizan estos datos para extraer porciones de información sobre las preferencias, gustos, y hábitos del usuario. También llevan a cabo una minería de datos para extraer información sobre un grupo; por ejemplo, el comportamiento de los adolescentes de una ciudad o región en particular. Las compañías de Internet pueden predecir con certeza lo que una persona con un determinado perfil compraría o haría. Este valioso bloque de datos sobre los usuarios de Internet tiene distintos usos comerciales, pero, ante todo, les sirve a los prestadores, quienes lo usan para realizar sus actividades de marketing.

Los asuntos

Protección de los usuarios y transparencia

En términos formales, al hacer clic en «acepto» bajo los comúnmente largos contratos de letra chica o los términos de servicio, los usuarios aceptan las condiciones impuestas por el proveedor de servicios. La pregunta es: ¿los usuarios comprenden su decisión, especialmente a la luz del potencial uso de sus datos con motivos comerciales? Es muy probable que – en muchos casos – los usuarios acepten el «trato» de intercambiar sus datos por los valiosos servicios de Internet sin considerarlo seriamente. Mientras más transparentes y fáciles de comprender son los acuerdos, más beneficios traen; no solo para los usuarios sino también para las compañías de Internet que pueden asegurar un modelo de negocio más sostenible, basado en las elecciones informadas de los usuarios de Internet.

Riesgo de abuso de las posiciones dominantes en el mercado

La industria de Internet es propensa a establecer monopolios de mercado. A modo de ejemplo, en agosto de 2016, Google se llevó el 70% del mercado de motores de búsqueda desde escritorios, y más del 90% para las búsquedas móviles/desde tablets.[24]

Cuando las compañías gozan de una posición monopólica (o dominante) en el mercado, tienden a abusarse de esas posiciones e imponen barreras que impiden o dificultan que nuevas compañías ingresen al mercado. Para abordar esos problemas, las autoridades nacionales y/o regionales deben tener a su disposición mecanismos de supervisión eficientes y efectivos, así como la habilidad de desarrollar y aplicar políticas y legislaciones de competencia adecuada y antimonopólica. Aunque dichas políticas y legislaciones son específicas para cada país o región, pueden emplearse para abordar eficientemente el comportamiento anticompetitivo de las compañías de Internet mundiales que operan a nivel local o regional. La UE, por ejemplo, debido a sus regulaciones de mercado avanzadas en esta área, ha realizado muchas iniciativas destinadas a evitar o abordar prácticas ilícitas, y a obligar a las compañías a cumplir con las regulaciones. En los últimos años, la Comisión Europea ha comenzado a mostrar un papel muy activo en el monitoreo de la competencia en el mercado digital de la UE. Consecuentemente, inició varias acciones contra el supuesto abuso de las compañías de Internet cuyas posiciones son dominantes en el mercado. Google fue el blanco de algunas de estas acciones, que se centraron, entre otras cosas, en las prácticas publicitarias de la compañía.

Economía de ACCESO a Internet

Los usuarios de Internet y las compañías les pagan a los PSI por los servicios relacionados con el acceso a Internet. Típicamente, los PSI tienen que cubrir los siguientes gastos con las tarifas que recaudan:

- Costos de los gastos de telecomunicaciones y ancho de banda de Internet para el siguiente núcleo de Internet más importante.
- Costos de las direcciones IP obtenidas desde los RIR o los LIR locales. Cada dispositivo que tenga acceso a Internet necesita una dirección de IP.
- Costos de adquisición, instalación, y mantenimiento del equipo y *software* (Figura 20).

Cada vez más, el negocio del acceso a Internet se ve más complejizado por los requisitos regulatorios del gobierno en áreas como la retención de datos. Que existan más regulaciones significa que habrá más gastos, que serán costeados por los usuarios de Internet mediante las tarifas de suscripción, o bien amortizadas con una menor ganancia para los PSI.

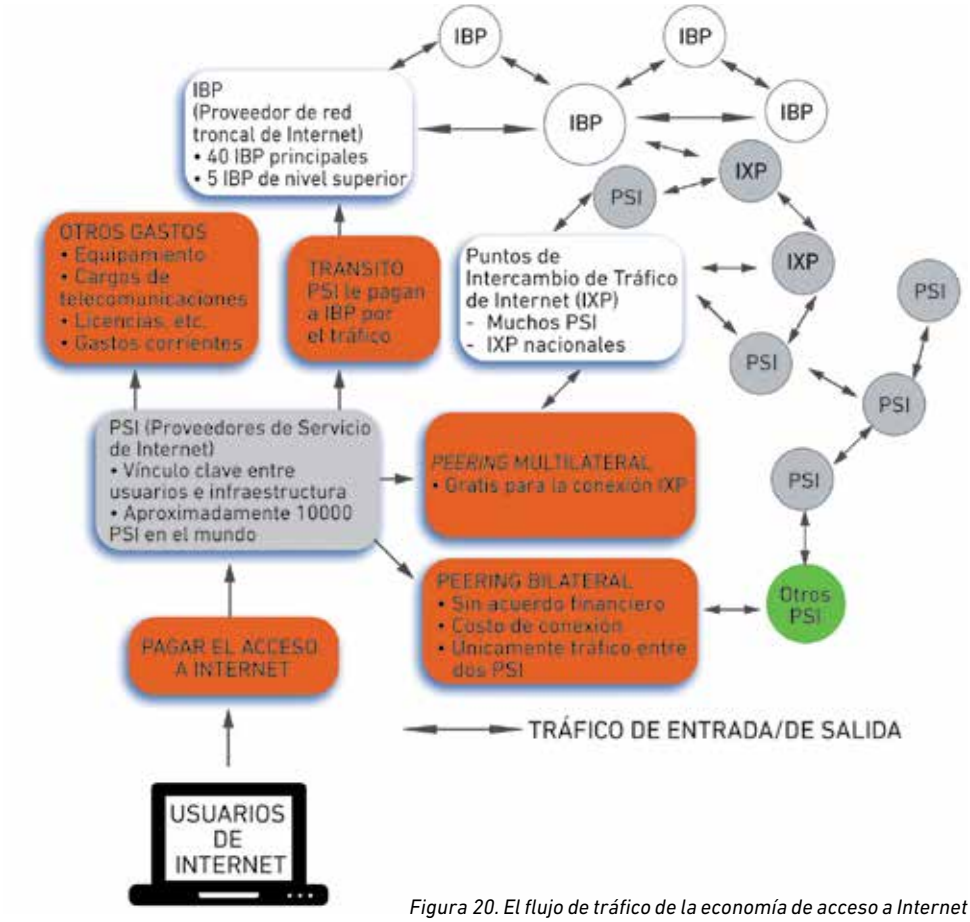

Figura 20. El flujo de tráfico de la economía de acceso a Internet

Los asuntos

Redistribución de las ganancias entre las compañías de telecomunicaciones y de Internet

Las operadoras de telecomunicaciones presentaron la cuestión de la redistribución de las ganancias generadas por Internet. Están tratando de aumentar su porcentaje de las ganancias generadas por el auge de Internet. Hasta ahora, los principales beneficiarios del negocio del auge de Internet son las compañías de contenido de Internet, debido a su modelo de negocio novedoso, basado en la publicidad en línea. Las compañías de telecomunicaciones argumentan que ellas también deberían beneficiarse, ya que facilitan el acceso al contenido de Internet mediante *sus* infraestructuras de telecomunicación.

La industria de las telecomunicaciones usualmente justifica solicitar un ingreso más alto proveniente de las ganancias generadas por Internet, por la necesidad de invertir en la modernización de la infraestructura de telecomunicación. Las compañías de contenido, por otra parte, aseveran que los proveedores de acceso cobran a sus usuarios finales el acceso a Internet, y que la razón principal de sus supuestos bajos ingresos se debe a su modelo de negocios obsoleto (tarifas «ilimitadas» como tarifa plana). Las operadoras de telecomunicaciones europeas, mediante la ETNO, dieron lugar a controversias durante la preparación de la CMTI-12 en Dubái, cuando propusieron que los proveedores de contenidos (por ejemplo, Facebook, Google) pagaran el acceso a sus servicios. Esta propuesta no consiguió mucho apoyo en ese momento, pero es posible que siga siendo un tema inconcluso en las futuras negociaciones en la gobernanza de Internet.

El debate sobre la redistribución de las ganancias de Internet respalda fuertemente el debate sobre la neutralidad de la red – por ejemplo, ¿todo el tráfico de Internet debería recibir el mismo tratamiento? ¿O debería ser segregado en distintos niveles, dependiendo de la calidad del servicio, pago, y confiabilidad? (Por ejemplo, un rango de opciones de una Internet VIP a una Internet para los menos privilegiados).

Tarifa plana vs pago por paquete

La discusión sobre tarifas planas de Internet suele estar enmarcada en términos de como lograr un equilibrio adecuado y óptimo entre tres aspectos: eficiencia técnica, eficiencia económica, y efectos sociales.[25] Algunos autores subrayan los desafíos de reemplazar la estructura de fijación de precios existente – simple y de tarifa plana – por una más compleja, como una contabilidad basada en el tráfico de paquetes.[26] En lo que respecta a los desafíos prácticos, algunos creen que cambiar las políticas tarifarias de Internet actuales podrían abrir una caja de Pandora, desencadenando más problemas que soluciones.

Compartir las ganancias de las telecomunicaciones con los países en desarrollo

Muchos países en vías de desarrollo plantearon la cuestión sobre la equidad de las condiciones económicas de la economía de Internet. Comparado con el sistema de telefonía tradicional, en el que el precio de cada llamada internacional se comparte entre los dos países, el modelo de Internet coloca toda la carga sobre uno de los lados: los usuarios en los países en desarrollo pueden tener que financiar la conexión a las redes troncales de Internet ubicadas principalmente en los países desarrollados. Como resultado, paradójicamente, los países pequeños y de menor riqueza terminan subsidiando la Internet en países desarrollados.

El problema del arreglo financiero tiene una particular relevancia para los países más pobres, que cuentan con los ingresos de las telecomunicaciones internacionales como importante fuente presupuestaria. La situación se complicó aun más con la introducción del VoIP – telefonía de Internet – que traslada el tráfico telefónico desde las operadoras de telecomunicaciones nacionales hacia la Internet.

Los países en vías de desarrollo pusieron de relieve la cuestión de un acceso a los modelos de negocio de Internet más justo en contextos múltiples, incluidos la CMSI, los grupos de trabajo de la UIT, y en la CMTI-12.

Tendencias emergentes: Internet de las Cosas, inteligencia artificial, economía colaborativa

La IoT es una tendencia emergente que está causando un impacto enorme sobre la economía de Internet. La integración de la IoT en los modelos de negocio reduce los costos y aumenta la eficiencia. Muchas empresas nuevas actualmente utilizan «edificios inteligentes» para optimizar los costos de energía y preservar el medio ambiente. La aplicación de soluciones TIC en los procesos de negocios crea empresas con una ventaja competitiva, que les ayuda a desarrollarse más rápidamente que en el entorno tradicional. Por lo tanto, las empresas ahora exigen enfoques nuevos, personalizados, e innovadores por parte de la industria de la TI, que contribuye bastante en el bienestar económico general.

También se espera que los avances en el campo de la IA produzcan efectos económicos significativos. Por un lado, la nueva ola de automatización que trae la IA posiblemente genere un crecimiento considerable de la productividad. Por el otro, surgieron inquietudes con respecto al impacto que podría causar esta automatización en los trabajos y el empleo.

El último modelo en la economía de Internet se denomina economía colaborativa, que catapultó a los nuevos jugadores – como Uber y Airbnb – hacia el mercado mundial. Estas empresas sacaron todo el provecho de las oportunidades que ofrecía la economía de Internet, por medio de la integración de soluciones digitales en sus procesos de negocio, apalancando así los costos reducidos de negocios, y mediante un acceso más directo a los consumidores. Al mismo tiempo, esos modelos se enfrentaron con la oposición de los negocios tradicionales, como los servicios de taxi y hotel. Todavía continúa la controversia sobre la necesidad de contar con regulaciones específicas para la economía colaborativa (es decir, para cubrir los temas de responsabilidad, protección del consumidor, cargas fiscales, etc.), e incluso hasta si los gobiernos deberían prohibir los servicios que estén dentro de esta categoría. La UE, hasta ahora, eligió mantener una «actitud expectante». La Comisión Europea publicó, en junio de 2016, un Comunicado sobre la Agenda Europea para la economía colaborativa, destinado a guiar a los estados miembros sobre qué legislación de la UE debería aplicarse a la economía colaborativa. La Comisión también sugirió que las prohibiciones absolutas para las actividades de la economía colaborativa deberían solamente constituir una medida de última instancia.[27]

Una consecuencia del comercio electrónico es el mercado de trabajadores independientes emergente. Por un lado, esto dio inicio a una vibrante comunidad inicial de trabajadores independientes y contribuyó en el fortalecimiento de las PyME y la reducción del

desempleo. Por otro lado, esto exige un nuevo enfoque hacia el trabajo, sobre todo debido al tratamiento del ingreso que surge del trabajo de los profesionales.

Otra área que contribuyó significativamente a la economía de Internet – y que al mismo tiempo fue la propulsión de numerosos debates – es la de las apuestas electrónicas. Se aplicaron a las apuestas electrónicas unos enfoques regulatorios diferentes, debido a sus características únicas. La UE, por ejemplo, la deja en manos de los estados miembros para que estos la regulen. La sensibilidad de esta área y su interrelación con las políticas públicas, la moral, la protección de menores, y los temas de delincuencia en la ciberseguridad pusieron de relieve que la regulación de las apuestas electrónicas es más adecuada para su elaboración a nivel nacional, dependiendo de los trasfondos políticos y sociales de cada país.

www.igbook.info/othereconomic

Banca electrónica, dinero electrónico, y monedas virtuales

El dinero digital es una amenaza para cada gobierno del planeta que quiera controlar su moneda.

David Saxton, cofundador de Net1[28]

Banca electrónica

La banca electrónica implica el uso de Internet para llevar a cabo operaciones bancarias convencionales, como el pago de tarjetas o la transferencia de fondos. Lo novedoso es únicamente el medio, ya que el servicio bancario sigue siendo esencialmente el mismo. La banca electrónica brinda ventajas a los clientes ofreciendo acceso en línea y opciones digitales, y reduciendo los costos de las transacciones. Por ejemplo, se estima que las transacciones de los clientes que cuestan 4 dólares estadounidenses en el banco tradicional, solamente cuestan 0,17 centavos de dólares en la banca electrónica.[29]

Dinero electrónico

El dinero electrónico o *e-money* en inglés es el balance de dinero registrado electrónicamente en una tarjeta de valor almacenado o de manera remota en un servidor. El Banco de Pagos Internacionales (BPI) define al dinero electrónico como «mecanismos de pago de valor almacenado o prepago para ejecutar pagos mediante terminales punto de venta, transferencias directas entre dos dispositivos, o incluso redes informáticas abiertas como Internet».[30] El dinero electrónico tiene su raíz en el sistema bancario y monetario existente (moneda corriente financiera supervisada por los bancos nacionales). Se lo asocia usualmente con las tarjetas inteligentes emitidas por compañías como Mondex y Visa Cash.

Moneda digital, moneda virtual, y moneda criptográfica

A diferencia del dinero electrónico que representa la moneda fiduciaria (como el euro o el dólar) sin cambiar su valor, la moneda digital no es equivalente a ninguna moneda fiduciaria (y no es parte de ningún sistema financiero; por lo tanto, no está regulada por las autoridades estatales).

Las monedas digitales pueden estar centralizadas o descentralizadas. En un modelo centralizado, las operaciones tales como la emisión de la moneda, y los mecanismos para implementar y hacer cumplir las reglas sobre el uso y la circulación de la moneda están gestionados por una parte central. En un modelo descentralizado, a estas operaciones las gestionan varias partes a lo largo de la red.

Tanto las monedas virtuales como las monedas criptográficas son tipos de monedas digitales. Mientras que las monedas virtuales están basadas en un modelo centralizado, las monedas criptográficas (monedas digitales que usan cifrado por motivos de seguridad, haciéndolas más difíciles de falsificar) pueden estar centralizadas o descentralizadas. La Bitcoin es un ejemplo de moneda criptográfica descentralizada.[31]

En 2012, el Banco Central Europeo definió al dinero virtual (monedas virtuales) como un «tipo de dinero no regulado y digital que se emite y, por lo general, se controla por quienes lo desarrollan, y lo usan y aceptan los miembros de una comunidad virtual específica».[32] En 2014, la Autoridad Bancaria Europea expresó que la moneda virtual es «una representación digital de valor que no es emitida por un banco central ni por una autoridad pública, ni tampoco está atada a una correspondencia fiduciaria, pero es aceptada por personas naturales o jurídicas como un medio de pago y puede ser transferida, almacenada o comercializada de manera electrónica».[33]

Bitcoin

El uso de Bitcoin se basa en tecnología de cadena de bloques, que significa que hay un registro central en todas las transacciones: una base de datos distribuida en una red informática (red P2P). Este *software* de código abierto permite que todos los pares en una red verifiquen cada transacción realizada en Bitcoin, y funcionan, así, como guardianes de este registro central. Los nodos (como se conoce a los pares en las redes) trabajan de manera colaborativa, interactuando poco y nada entre sí, por lo que adoptan una verificación mutua como prueba de la cronología de la transacción. Este «registro» es seguro siempre y cuando todo el poder informático (procesador) de los nodos honestos sea más alto que el de los deshonestos.

El número de bitcoins por producir tiene un límite de 21 millones, lo que significa que el valor de la moneda digital aumenta con el tiempo (los que la adopten antes, por lo tanto, se verán beneficiados). Cualquiera puede crear («minar») la Bitcoin: deben transmitir la solución de un problema matemático-computacional que jamás haya sido resuelto (utilizando el sistema de prueba de funcionamiento). Todos los nodos intentan resolver este «problema», y una vez encontrada la solución, ese bloque se cierra y todos los nodos avanzan hacia el siguiente problema (el siguiente bloque de la cadena). Los nodos, o «mineros» como se los llama, son recompensados por dedicar su poder informático a la seguridad de la red. Esta recompensa es un número específico de bitcoins y tarifas de transacción que costearán terceros.

Las monedas criptográficas están configuradas para llevarse el mundo digital por delante, debido a que su popularidad y uso van en aumento. Grandes compañías como Apple, Dell, y PayPal ya mencionaron sus planes de incorporar las monedas criptográficas como un medio de pago, y muchas más posiblemente hagan lo mismo.

En los últimos años, la Bitcoin emergió como una de las monedas criptográficas más populares, y el número de servicios que admiten su uso creció dramáticamente.

Las principales ventajas de las monedas criptográficas son las bajas tarifas en comparación con el sistema bancario tradicional, los pagos rápidos y transparentes, y el acceso móvil. Estas ventajas pueden propulsar las actividades de *start-up* y ayudar a los países en desarrollo a llegar a una igualdad de condiciones con respecto a los países desarrollados en el mercado global.

Muchos servicios mundiales ahora aceptan a la Bitcoin como medio de pago, y estas transacciones han quedado exentas del impuesto al valor agregado (IVA) en varios países. En julio de 2015, el TJUE sentenció que el cambio de una moneda tradicional por Bitcoin en línea debería estar exento de impuestos de consumo como otras transacciones de billetes y monedas.

También parece que los bancos centrales están prestando cada vez más atención a las monedas virtuales. A modo de ejemplo, a principios de 2016, el Banco Popular de China anunció que estaba investigando la posibilidad de lanzar su propia moneda virtual, considerándolo como una contribución en la transparencia de las actividades económicas, y en la reducción de lavado de dinero y evasión impositiva.[34]

En 2016, el Fondo Monetario Internacional (FMI) publicó el informe Las monedas virtuales y más allá: Consideraciones iniciales. El informe señala los diferentes desafíos en relación con la regulación y elaboración de políticas de las monedas virtuales, como la protección del consumidor, las cargas fiscales, y la estabilidad financiera. Según este informe, las respuestas políticas adecuadas «deberán calibrar la regulación de manera tal que se enfrenten adecuadamente los riesgos sin estancar la innovación». A nivel internacional, las mejores prácticas y los estándares internacionales deberían guiar las respuestas políticas y promover la armonización de las jurisdicciones.[35]

Los asuntos

Cambios en el sistema bancario mundial

El incrementado uso de la banca electrónica y el dinero electrónico podría causar cambios en el sistema bancario mundial, brindándoles a los clientes nuevas posibilidades y reduciendo los gastos bancarios. Los métodos bancarios tradicionales se verán desafiados por la banca electrónica, de mayor rentabilidad. Cabe mencionar que la mayoría de los bancos convencionales han adoptado la banca electrónica. En 2002, solamente 30 bancos brindaban servicios en línea en EE. UU. Hoy en día, es difícil encontrar un banco que no opere con los servicios de banca electrónica.

Comercio móvil

Los pagos y el dinero electrónico están, actualmente, atravesando cambios acelerados, junto con la evolución y el desarrollo de la tecnología y los dispositivos. Los pagos móviles ya sobrepasaron las simples órdenes hechas a través de SMS, debido a que los teléfonos móviles se vuelven más sofisticados e «inteligentes» (como los teléfonos *smart* y los iPhones) y dan lugar a distintas aplicaciones, incluido el comercio móvil.

Ciberseguridad

La ciberseguridad es uno de los principales retos en el desarrollo amplificado de los pagos electrónicos. ¿Cómo se puede asegurar la protección de las transacciones financieras a través de Internet? Es importante remarcar la responsabilidad de los bancos y otras instituciones financieras con respecto a la seguridad de las transacciones en línea. El principal desarrollo en este sentido fue la Ley Sarbanes-Oxley (SOX),[36] promulgada por el Congreso de EE. UU. como reacción ante los escándalos financieros de Enron, Arthur Andersen, y WorldCom. Esta ley hace más estricto el control financiero e incrementa la responsabilidad de las instituciones financieras en relación con la seguridad de las transacciones en línea. También reparte la carga de la responsabilidad de la seguridad entre los clientes – quienes deben demostrar cierta prudencia – y las instituciones financieras.

Falta de disponibilidad de métodos de pago electrónico

La indisponibilidad de métodos de pago electrónico generalmente es uno de los principales impedimentos para un desarrollo más rápido del comercio electrónico. Actualmente, el comercio electrónico se lleva a cabo principalmente mediante tarjetas de crédito. Este es un obstáculo importante para los países en vías de desarrollo que no han desarrollado un mercado con tarjetas de crédito. Los gobiernos en estos países tendrían que promulgar cambios jurídicos para habilitar la rápida introducción de los pagos mediante tarjetas.

Iniciativas nacionales y regionales

Para fomentar el desarrollo del comercio electrónico, los gobiernos de todo el mundo necesitan incentivar todas las formas de pago que no sean mediante el efectivo, como las tarjetas de crédito y el dinero electrónico. La introducción acelerada del dinero electrónico requerirá más actividades regulatorias gubernamentales.

Después de Hong Kong, primera ciudad en introducir una legislación integral sobre el dinero electrónico, la UE publicó la Directiva sobre Dinero Electrónico en 2000 (modificada en 2009).[37] A diferencia del dinero electrónico, todavía no existe regulación para la moneda digital y/o virtual en la UE. Actualmente, queda en manos de los estados miembros regular las monedas como Bitcoin. Alemania considera que la Bitcoin es «dinero privado» que se utiliza en transacciones entre dos personas o entidades. En el Reino Unido, es considerada un tipo de cambio, pero no dinero. La mayoría de los países han escogido una postura «expectante» con respecto a esto. Otros países, como Rusia y Tailandia, dieron pasos más radicales para prohibir las transacciones mediante Bitcoin a nivel nacional.

Iniciativas internacionales

Gracias a la naturaleza de Internet, es posible que el dinero electrónico y las monedas virtuales se conviertan en un fenómeno global, lo que brinda una razón para abordar este tema a nivel internacional. Un jugador potencial en el campo de la banca electrónica es el Grupo de Banca Electrónica del Comité de Basilea. Este grupo ya comenzó a abordar la autorización, estándares de prudencia, transparencia, privacidad, lavado de dinero, y la supervisión transfronteriza, que son asuntos clave para la introducción del dinero electrónico.[38]

La principal iniciativa internacional con respecto a la moneda virtual tomó forma en la Fuerza de Trabajo de Acción Financiera (FATF, por sus siglas en inglés), que aborda las cuestiones del lavado de dinero y la financiación del terrorismo. Los Estados Unidos

iniciaron un debate en la FATF sobre cómo aplicar reglas en contra del lavado de dinero y la financiación del terrorismo en el campo de las monedas virtuales.

El vínculo de la aplicación de la ley

La petición de 2002 del Fiscal General del Estado de Nueva York a PayPal y Citibank para que no ejecutaran los pagos a casinos de Internet es un ejemplo de cómo las agencias de aplicación de la ley comenzaron a hacer uso de los sistemas de pago electrónico para llevar a cabo sus tareas.[39] Lo que no pudo lograr la aplicación de la ley mediante mecanismos legales, se consiguió mediante el control de los pagos electrónicos.

Privacidad

Cada transacción de pago electrónico deja un rastro, que registran los emisores del instrumento de pago electrónico (las compañías de tarjetas de crédito, los bancos). Aunque contar con este registro es necesario y justificable para mantener las cuentas claras y la evidencia de los pagos, la acumulación de esos datos puede representar una grave amenaza a la privacidad de los usuarios cuando se usa la minería de datos para rastrear los hábitos de compras y gastos, o para marcar a los clientes para la prestación de futuros servicios financieros.

Riesgos y uso indebido de las monedas virtuales

El riesgo de la moneda virtual quedó en claro tras el cierre de Mt Gox, uno de los mercados de cambio más grandes en línea de Bicoin, en febrero de 2014.[40] Sus varios inversores perdieron cerca de 500 millones de dólares en un caso de robo de las credenciales de la cuenta de un usuario.

Muchas advertencias indican que las monedas virtuales podrían potencialmente ser usadas de manera indebida en bienes y servicios ilegales, fraude, y lavado de dinero. El anonimato de las transacciones criptográficas de Bitcoin aumenta el potencial del uso indebido. Además, los monederos Bitcoin (lugar en el que se almacenan las Bitcoins fuera de línea) también pueden estar cifrados.

En 2014, la FBI cerró el sitio web de la Ruta de la Seda, que se utilizaba para comercializar datos de tarjetas robadas, drogas, y otros productos ilegales; el sitio web usaba Bitcoins como medio de pago.[41]

Un informe financiado por el gobierno de EE. UU. sobre las Implicancias de las Monedas Virtuales para la Seguridad Nacional, publicado a fines del 2015, indicó que los «actores no estatales», incluidos los terroristas y grupos insurgentes, pueden explotar la moneda virtual usándola en transacciones económicas ordinarias.[42]

La UE está tratando de abordar estos problemas a través de medidas legislativas. En julio de 2016, la Comisión Europea publicó una propuesta para enmendar la Directiva sobre la prevención del uso del sistema financiero para el lavado de dinero o la financiación del terrorismo. La propuesta tiene como objetivo, entre otras cosas, poner a las plataformas de cambio de moneda virtual bajo la lupa de la Directiva, exigiéndoles que introduzcan medidas de control de diligencia debida que ayudarían en la detección de transacciones sospechosas de monedas virtuales. Esta propuesta también pretende introducir una definición jurídica de las monedas virtuales, y utiliza, a tal fin, la definición proporcionada por la Autoridad Bancaria Europea en 2014.[43]

www.igbook.info/emoney

Protección del consumidor

La confianza del consumidor es uno de los requisitos previos más importantes para que el comercio electrónico sea exitoso. Este es todavía relativamente nuevo y los consumidores no confían tanto en él como lo hacen en las compras en el mundo real. La protección del consumidor es un método legal importante para el desarrollo de la confianza en el comercio electrónico. La regulación del comercio electrónico debería proteger a los consumidores en varias áreas, como:

- Manejo en línea de la información de la tarjeta de pago.
- Publicidad engañosa.
- Entrega de productos defectuosos.

Una característica nueva específica del comercio electrónico es la internacionalización de la protección del consumidor, que no es un problema crucial en el comercio tradicional. Anteriormente, los consumidores rara vez necesitaban una protección del consumidor local. Compraban de manera local y, por lo tanto, necesitaban una protección del consumidor local. En el caso del comercio electrónico, se lleva a cabo un creciente número de transacciones internacionales.

La jurisdicción es un tema importante que rodea a la protección del consumidor. Involucra dos enfoques principales. El primero favorece al vendedor (principalmente empresas electrónicas) y es un enfoque basado en el país de origen establecido por el vendedor. En este contexto, las compañías de comercio electrónico tienen la ventaja de contar con su propio entorno jurídico, que es predecible y conocido. El otro enfoque, que favorece al consumidor, está basado en el país de destino.

La principal desventaja para las compañías de comercio electrónico es que están potencialmente expuestas a una amplia variedad de jurisdicciones legales. Una posible solución para este dilema es la mejor armonización de las reglas de protección del consumidor, lo que haría menos relevante la cuestión de la jurisdicción. Al igual que con otros problemas del comercio electrónico, la OCDE tomó la delantera al elaborar las Directrices para la Protección del Consumidor en el Contexto del Comercio Electrónico[44] de 1999 y las Directrices de la OCDE para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas de 2003.[45] Los principios más importantes establecidos por la OCDE son aún válidos y fueron adoptados por otras asociaciones de negocios, incluida la CCI.

La UE ofrece un alto nivel de protección del consumidor en el comercio electrónico y promueve campañas de concientización sobre los temas de las compras en línea. Al problema de la jurisdicción lo abordó el Reglamento Bruselas I,[46] que estipula que los consumidores siempre tendrán la posibilidad de recurrir a la protección legal local. La refundición del Reglamento Bruselas I,[47] en vigencia desde enero de 2015, armoniza un poco más las reglas de jurisdicción al extender las situaciones en que los individuos no domiciliados en la UE pueden ser demandados por los consumidores en los tribunales de los estados miembros de la UE.

Una serie de asociaciones privadas y ONG también se centran en la protección del consumidor en el área del comercio electrónico, incluidas Consumers International, International Consumer Protection and Enforcement Network, y la CCI.

El futuro desarrollo del comercio electrónico exigirá la (mayor) armonización de las leyes nacionales o un nuevo régimen internacional para la protección del consumidor en el comercio electrónico.

www.igbook.info/consumers

Cargas fiscales

El espíritu de la discusión sobre la Internet y las cargas fiscales puede ser comparado con la respuesta de Faraday a un político escéptico que le preguntó acerca del propósito de su invención (inducción electromagnética). «Señor, no sé para qué sirve. Pero hay algo de lo que sí estoy seguro: algún día usted va a cobrar impuestos por esto».[48]

Mientras más se ubica la Internet en el centro de la economía moderna, más atención va dirigida a la cuestión de las cargas fiscales. Esto se ha vuelto incluso más importante tras la crisis financiera en 2008. Muchos gobiernos han tratado de elevar sus ingresos fiscales para reducir la creciente deuda pública. Las cargas fiscales de las actividades económicas en Internet se convirtieron en una de las primeras posibilidades para el aumento del ingreso fiscal.

Uno de los primeros informes completos sobre las cargas fiscales en Internet fue el del Ministerio francés de Economía y Finanzas en enero de 2013,[49] seguido por otros informes sobre el tema de las cargas fiscales en la economía digital.[50]

El dilema de la gobernanza de Internet acerca de tratar a los problemas cibernéticos de manera diferente de los de la vida real se refleja en el asunto de las cargas fiscales. Desde el comienzo, EE. UU. ha estado intentando declarar a Internet como una zona libre de impuestos. En 1998, el Congreso de EE. UU promulgó la Ley Permanente para una Internet Libre de Impuestos. Después de que la aplicabilidad de esta ley se extendiera varias veces, en 2016 el Congreso de EE. UU. aprobó una legislación que prohíbe permanentemente que los estados y los gobiernos impongan cargas fiscales para el acceso a Internet. Además de la extensión permanente de esta ley, la medida también prohíbe los impuestos a los bienes y servicios digitales.[51]

La OCDE y la UE promovieron el punto de vista de que la Internet no debería tener un tratamiento impositivo especial. Los Principios de Ottawa de la OCDE de 1998 especifican que la carga impositiva del comercio electrónico debería estar basada en los mismos principios que para las cargas impositivas de las actividades del comercio tradicional: neutralidad, eficiencia, claridad y simplicidad, eficacia y equidad, y flexibilidad.[52] En un informe de 2014, la Comisión Europea reitera que «no debería existir un régimen impositivo especial para las compañías digitales. En cambio, deberían aplicarse o adaptarse las reglas generales para que las compañías "digitales" reciban el mismo tratamiento que las otras».[53]

Desde la perspectiva de que la Internet no debería recibir tratamiento impositivo especial, la UE introdujo una regulación en 2003 que solicitaba que las compañías de comercio electrónico no pertenecientes a la UE abonaran IVA cuando vendieran productos dentro de la UE. La principal motivación de la decisión de la UE fue que las compañías que no pertenecían a la UE (más que nada, de EE. UU.) tenían una ventaja sobre las compañías europeas, que tenían que abonar IVA en todas las transacciones, incluidas las electrónicas.

Actualmente, los países no europeos han comenzado a adoptar la misma estrategia. Debido al rápido incremento en la cantidad de usuarios de Internet y la aumentada centralidad de las compañías de Internet – principalmente de EE. UU. – en sus economías, muchos países han comenzado a cobrar impuestos a los servicios de Internet que ofrecen compañías no registradas dentro de sus territorios. Los ejemplos van desde Rusia[54] y la India[55], hasta Israel[56] e Indonesia[57].

Otra arista de las cargas fiscales electrónicas que permanece sin solución es la de la ubicación de estas cargas. Los Principios de Ottawa introdujeron un principio de «destino» en lugar de «origen» de las cargas fiscales. El gobierno de EE. UU., sin embargo, está muy interesado en hacer que las cargas fiscales permanezcan en el origen de las transacciones, debido a que la mayoría de las compañías de comercio electrónico están basadas en EE.UU. Por el contrario, la UE, por ejemplo, está interesada en imponer las cargas fiscales en el destino, ya que posee más consumidores de comercio electrónico que vendedores.

En el contexto de Internet, el asunto de las cargas fiscales no se debate solamente como un objeto de legislación revisada, sino también en el contexto de evasión de impuestos de grandes compañías de Internet. En enero de 2016, la Comisión Europea presentó un Paquete de Lucha contra la Elusión Fiscal, que tiene la finalidad de evitar que las compañías en la UE trasladen sus ganancias a los países de bajos impuestos. La publicación llegó en medio de las discusiones relativas a las prácticas impositivas de Google. Según autoridades italianas, Google evadió impuestos por 227 millones de euros entre 2009 y 2013.[58] Además de esto, en el Reino Unido se generó una controversia sobre la revelación de un acuerdo impositivo de 130 millones de libras esterlinas entre Google y las autoridades fiscales nacionales.[59] En mayo de 2016, el gobierno francés incluso organizó un allanamiento en la sede parisina de Google como parte de una investigación de fraude impositivo, debido a que Francia acusó a la compañía de deber 1,6 mil millones de euros por impuestos impagos.[60] Un estudio reciente llevado a cabo por el *Interest Research Group Education Fund* y por *Citizens for Tax Justice* demostró que entre las 30 empresas más evasoras de impuestos, 10 eran compañías tecnológicas, encabezadas por Apple.[61]

Algunos países introducen exenciones impositivas para los proveedores de infraestructura y/o los proveedores de servicios en línea, con el objetivo de incentivar las inversiones en el desarrollo de la infraestructura, y de impulsar compañías de comercio electrónico locales. En la India, por ejemplo, el ministerio de telecomunicaciones propuso unas «vacaciones» impositivas de 10 años para los grandes proyectos en el sector de la TI para motivar las inversiones.[62] En China, el Consejo de Estado ofrece concesiones impositivas para las compañías chinas de alta tecnología, en las que bajan sus impuestos empresariales del 25 al 15%.[63] El gobierno del Reino Unido incorporó una disposición en el presupuesto de 2016 que introduce una exención de impuestos para los microemprendedores que venden sus servicios en línea o que rentan sus hogares mediante Internet.[64]

www.igbook.info/taxation

NOTAS FINALES

1 Andrew Odlyzko analiza la cuestión de los precios y la arquitectura de Internet desde una perspectiva histórica. Andrew establece una relación entre el hilo de la política de fijación de precios de los sistemas de transporte en la antigüedad y la política de fijación de precios actual para Internet. Para obtener más información, consulte: Odlyzko A (2004) Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation. Disponible en http://www.dtc.umn.edu/~odlyzko/doc/pricing.architecture.pdf [accedido el 25 de octubre de 2016].

2 Banco Mundial (2016) Informe de Desarrollo Mundial 2016: Dividendos Digitales. Disponible en http://www.worldbank.org/en/publication/wdr2016 [accedido el 29 de octubre de 2016].

3 La Casa Blanca (1997) Marco para el Comercio Electrónico Global. Disponible en https://clinton4.nara.gov/WH/New/Commerce/ [accedido el 25 de octubre de 2016].

4 OMC (1998) Programa de Trabajo sobre el Comercio Electrónico. Disponible en http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm [accedido el 25 de octubre de 2016].

5 Unión Europea (2000) Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). Disponible en http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32000L0031 [accedido el 25 de octubre de 2016].

6 PFSweb (2015) B2B eCommerce. Disponible en http://www.pfsweb.com/PDF/whitepapers/PFSweb-B2B-eCommerce-Whitepaper.pdf [accedido el 16 de agosto de 2016].

7 OMC (sin fecha) El GATT y el Consejo del Comercio de Mercancías Disponible en https://www.wto.org/english/tratop_e/gatt_e/gatt_e.htm [accedido el 25 de octubre de 2016].

8 OMC (sin fecha) Comercio de servicios. Disponible en https://www.wto.org/english/tratop_e/serv_e/serv_e.htm [accedido el 2 de noviembre de 2016].

9 OMC (1994) Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio. Disponible en https://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm [accedido el 25 de octubre de 2016].

10 Si bien era «temporaria», la moratoria ha sido extendida posteriormente por la Conferencia Ministerial de la OMC. La decisión más reciente en este sentido tuvo lugar en la Conferencia Ministerial en Nairobi en diciembre de 2015, y será revisada en la conferencia de 2017. Consulte la Conferencia Ministerial de la OMC (2015) Decisión Ministerial del 19 de diciembre de 2015: WT/MIN(15)42 – WT/l/977. Disponible en https://www.wto.org/english/thewto_e/minist_e/mc10_e/l977_e.htm [Accedido el 25 de octubre de 2016].

11 Para obtener más detalles sobre las actividades relacionadas con el comercio electrónico, consulte: OMC (sin fecha) Comercio electrónico. Disponible en http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm [accedido el 25 de octubre de 2016].

12 Para obtener más información sobre el caso de apuestas en línea de EE.UU./Antigua, consulte https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm [accedido el 25 de octubre de 2016].

13 Geneva Internet Platform (2016) Informe del Foro Público de la OMC 2016. Disponible en http://digitalwatch.giplatform.org/events/wto-public-forum [accedido el 27 de octubre de octubre de 2016].

14 Para obtener una revisión más completa sobre los debates acerca del comercio electrónico dentro de la OMC, consulte: Maciel M (2016) E-commerce in the WTO: the next arena of Internet policy discussions. Disponible en https://www.diplomacy.edu/blog/e-commerce-wto-next-arena-Internet-policy-discussions [accedido el 27 de octubre de 2016].

15 CMUDMI (1996) Ley Modelo sobre el Comercio Electrónico. Disponible en http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html [accedido el 25 de octubre de 2016].

[16] Asamblea General de las Naciones Unidas (2005) Resolución A/60/20. Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales. Disponible en http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html [accedido el 2 de noviembre de 2016].

[17] Sitio web ebXML. Disponible en http://www.ebxml.org/ [accedido el 25 de octubre de 2016].

[18] UNCTAD (sin fecha) Informe sobre la Economía de la Información (serie). Disponible en http://unctad.org/en/Pages/Publications/InformationEconomyReportSeries.aspx [accedido el 25 de octubre de 2016].

[19] UNCTAD (sin fecha) eTrade for All: Unlocking the Potential of E-Commerce in Developing Countries. Disponible en http://unctad.org/en/Pages/DTL/STI_and_ICTs/eTrade-for-All.aspx [accedido el 27 de octubre de 2016].

[20] OCDE (1998) Plan de Acción para el Comercio Electrónico. Disponible en http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=SG/EC(98)9/FINAL&docLanguage=En [accedido el 27 de octubre de 2016].

[21] Teleanu S (2016) Digital policy issues emphasised at the G20 Leaders' Summit. Disponible en https://www.diplomacy.edu/blog/digital-policy-issues-emphasised-g20-leaders'-summit [accedido el 27 de octubre de 2016].

[22] APEC (sin fecha) Paperless Trading Individual Action Plan. Disponible en http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Paperless-Trading-Individual-Action-Plan.aspx [accedido el 25 de octubre de 2016].

[23] COMESA (2010) Model Law on Electronic Transactions and Guide to enactment. Disponible en http://programmes.comesa.int/attachments/article/166/COMESA%20Model%20Law%20and%20%20Guide%20to%20Enactment%20(fin).pdf [accedido el 25 de octubre de 2016].

[24] Net Market Share (2016) Market Share Statistics for Internet Technologies. Disponible en https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0 [accedido el 1 de septiembre de 2016].

[25] Thuy T, Nguyen T yArmitage GJ (2005) Evaluating Internet Pricing Schemes: A Three-Dimensional Visual Model. *ETRI Journal* 27(1) pp. 64–74. Disponible en http://etrij.etri.re.kr/etrij/journal/article/article.do?volume=27&issue=1&page=64 [accedido el 25 de octubre de 2016].

[26] Hayel Y, Maille P y Tuffin B (2005) Modelling and analysis of Internet pricing: introduction and challenges. In Proceedings of the International Symposium on Applied Stochastic Models and Data Analysis (ASMDA), Brest, Francia. Disponible en http://conferences.telecom-bretagne.eu/asmda2005/IMG/pdf/proceedings/1389.pdf [accedido el 26 de octubre de 2016].

[27] Comisión Europea (2016) Una Agenda Europea para la Economía Colaborativa. Disponible en http://ec.europa.eu/DocsRoom/documents/16881 [accedido el 1 de septiembre de 2016].

[28] Citado en Holland K y Cortese A (1995) The future of money: e-cash could transform the world's financial life. *Bloomberg*, 12 de junio. *Business Week*, 12 June, p. 66.

[29] Como informa Olson T (2012) en Higher costs, new laws mean no more free rides on some bank services, accounts. *Pittsburgh Tribune-Review*, 1 de abril. Disponible en http://triblive.com/x/pittsburghtrib/business/s_789300.html [accedido el 1 de noviembre de 2016].

[30] Comité de Supervisión Bancaria de Basilea (1998) Risk Management for Electronic Banking and Electronic Money Activities. Basilea, marzo de 1998. Disponible en http://www.bis.org/publ/bcbs35.pdf [accedido el 25 de octubre de 2016]. Versión final publicada en 2003, disponible en http://www.bis.org/publ/bcbs98.htm [accedido el 25 de octubre de 2016].

[31] Kamberi A (2014) Cryptocurrencies and bitcoin. Disponible en http://www.diplomacy.edu/blog/cryptocurrencies-and-bitcoin [accedido el 25 de agosto de 2016].

[32] Banco Central Europeo (2012) Virtual currency schemes. Disponible en https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [accedido el 17 de agosto de 2016].

[33] Autoridad Bancaria Europea (2014) EBA Opinion on 'virtual currencies'. Disponible en https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf [accedido el 17 de agosto de 2016].

[34] *The Register* (2016) China to set up its own virtual currency. 22 de enero. Disponible en http://www.theregister.co.uk/2016/01/22/china-virtual-currency-risks/ [accedido el 29 de octubre de 2016].

[35] He D *et al.* (2016) Las monedas virtuales y más allá: Consideraciones iniciales. Discusión del personal del Fondo Monetario Internacional Nota 16/03. Disponible en https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf [accedido el 21 de febrero de 2016].

[36] *Soxlaw* (sin fecha) A guide to the Sarbanes Oxley Act. Disponible en http://www.soxlaw.com/ [accedido el 26 de octubre de 2016].

[37] Unión Europea (2009) del Parlamento Europeo y del Consejo de 16 de septiembre de 2009 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE. Disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF [accedido el 26 de octubre de 2016].

[38] El Grupo de Basilea tiene sede central en el Banco de Pagos Internacionales. Elabora un *Estudio de los desarrollos en el dinero electrónico e Internet y los pagos móviles*. Disponible en http://www.bis.org/publ/cpss62.pdf [accedido el 26 de octubre de 2016].

[39] Richtel M (2002) PayPal and New York in Accord on Gambling. *The New York Times*, 22 de agosto. Disponible en http://www.nytimes.com/2002/08/22/business/technology-paypal-and-new-york-in-accord-on-gambling.html?src=pm [accedido el 26 de octubre de 2016].

[40] Takemoto Y y Knight S (2014) Mt. Gox file for bankruptcy, hit with lawsuit. *Reuters*, 28 de febrero. Disponible en http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228 [accedido el 26 de octubre de 2016].

[41] Oficina Federal de Investigaciones (2014) Comunicado de Prensa: Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court. Disponible en http://www.fbi.gov/newyork/press-releases/2014/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court [accedido el 26 de octubre de 2016].

[42] Baron J *et al.* (2015) National Security Implications of Virtual Currency. Examining the Potential for Non-state Actor Deployment. Rand Corporation. Disponible en http://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1231/RAND_RR1231.pdf [accedido el 17 de agosto de 2016].

[43] Comisión Europea (2016) Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica la Directiva 2009/101/CE. Disponible en http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf [accedido el 17 de agosto de 2016].

[44] OCDE (1999) Directrices para la Protección del Consumidor en el Contexto del Comercio Electrónico. Disponible en http://www.oecd.org/Internet/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm [accedido el 26 de octubre de 2016].

[45] OCDE (2003) Directrices de la OCDE para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas Fraudulentas y Engañosas. Disponible en http://www.oecd-ilibrary.org/industry-and-services/oecd-guidelines-for-protecting-consumers-from-fraudulent-and-deceptive-commercial-practices-across-borders_9789264103573-en-fr [accedido el 1 de noviembre de 2016].

[46] Unión Europea (2001) Reglamento (CE) No 44/2001 (Reglamento Bruselas I). Disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:en:HTML [accedido el 26 de octubre de 2016].

[47] Unión Europea (2012) Reglamento (UE) No 1215/2012 (Refundición del Reglamento Bruselas I). Disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:en:PDF [accedido el 26 de octubre de 2016].

[48] Soete L y Weel B (1999) Cybertax. Maastricht Economic Research Institute on Innovation and Technology (MERIT), Maastricht University. Disponible en http://www.merit.unu.edu/publications/rmpdf/1998/rm1998-020.pdf [accedido el 27 de octubre de 2016].

[49] Collin P y Colin N (2013) Mission d'expertise sur la fiscalité de l'économie numérique. Disponible en http://www.economie.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf [accedido el 27 de octubre de 2016].

[50] Algunos ejemplos de publicaciones que abordan el tema de las cargas fiscales en Internet son: EY (2015) The dawning of digital economy taxation. Disponible en http://www.ey.com/Publication/vwLUAssets/ey-the-dawning-of-digital-economy-taxation/$FILE/ey-the-dawning-of-digital-economy-taxation.pdf [accedido el 17 de agosto de 2016]; Andes S y Atkinson R (2013) A Policymakers' Guide to Internet Tax. Dsiponible en http://www2.itif.org/2013-policymakers-guide-Internet-tax.pdf [accedido el 17 de agosto de 2016]; OCDE (2015) Cómo abordar los desafíos fiscales en la economía digital. Disponible en http://www.oecd-ilibrary.org/taxation/addressing-the-tax-challenges-of-the-digital-economy_9789264218789-en [accedido el 17 de agosto de 2016]. Para obtener más información sobre este tema, consulte el observatorio de GIP Digital Watch (sin fecha). Taxation. Disponible en http://digitalwatch.giplatform.org/issues/taxation [accedido el 17 de agosto de 2016].

[51] Phillips Erb K (2016) Congress Makes Internet Access Tax Ban Permanent. *Forbes*, 11 de febrero. Disponible en http://www.forbes.com/sites/kellyphillipserb/2016/02/11/congress-makes-internet-access-tax-ban-permanent/#a403c12380a3 [accedido el 26 de octubre de 2016].

[52] Los Principios de Ottawa son: Neutralidad, Eficiencia, Claridad y simplicidad, Eficacia y equidad, Flexibilidad. Vea OCDE (2003) Implantación del Marco Tributario de la Conferencia de Ottawa. Informe de 2003. Disponible en http://www.oecd.org/tax/administration/20499630.pdf [accedido el 26 de octubre de 2016].

[53] Comisión Europea (2014) Grupo de Expertos de la Comisión en materia de fiscalidad en la economía digital. Bruselas: Comisión Europea, p. 5. Disponible en http://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/taxation/gen_info/good_governance_matters/digital/report_digital_economy.pdf [accedido el 4 de julio de 2016].

[54] *The Moscow Times* (2016) Russia State Duma passes 'Google Tax Law. 15 de junio. Disponible en http://www.themoscowtimes.com/news/article/russia-state-duma-passes-google-tax-law/572693.html [accedido el 4 de julio de 2016].

[55] Revanna H (2016) Govt notifies 6% equalization tax on online advertisements. *IBT*, 31 de mayo. Disponible en http://www.ibtimes.co.in/govt-notifies-6-equalisation-tax-digital-ads-take-effect-june-1-680785 [accedido el 4 de julio de 2016].

[56] *The Guardian* (2016) Google, Facebook, eBay and other tech firms targeted by new Israeli tax rules. 12 de abril. Disponible en https://www.theguardian.com/technology/2016/apr/11/google-facebook-ebay-tech-firms-israel-tax [accedido el 4 de julio de 2016].

[57] *Reuters* (2016) Indonesia says Internet giants need to pay tax or face blockages. 29 de febrero. Disponible en http://www.reuters.com/article/us-indonesia-tax-Internet-idUSKCN0W20QM [accedido el 4 de julio de 2016].

[58] *Reuters* (2016) Italian tax police believe Google evaded 227 million euros in taxes: sources. 28 January. Disponible en http://uk.reuters.com/article/us-google-italy-tax-idUKKCN0V614L [accedido el 4 de julio de 2016].

[59] Robertson J (2016) Google tax row: what's behind the deal. *BBC News*, 28 de enero. Disponible en http://www.bbc.com/news/business-35428966 [accedido el 4 de julio de 2016].

[60] *BBC* (2016) Google's Paris HQ raided in tax probe. 24 de mayo. Disponible en http://www.bbc.com/news/business-36370628 [accedido el 4 de julio de 2016].

[61] McIntyre RS *et al*. (2015) Offshore Shell Games 2015. Disponible en http://www.uspirg.org/sites/pirg/files/reports/USP%20ShellGames%20Oct15%201.3.pdf [accedido el 4 de julio de 2016].

[62] Aulakh G (2016) Budget 2016: Telecom Ministry seeks 10-year tax holiday for Make in India drive. *Economic Times*, 15 de febrero. Disponible en http://economictimes.indiatimes.com/industry/telecom/budget-2016-telecom-ministry-seeks-10-year-tax-holiday-for-make-in-india-drive/articleshow/50988028.cms [accedido el 4 de julio de 2016].

[63] Ren (2016) Beijing offers tax concessions to hi-tech companies. *South China Morning Pos*t, 14 de febrero. Disponible en http://www.scmp.com/news/china/policies-politics/article/1913172/beijing-offers-tax-concessions-high-tech-companies [accedido el 4 de julio de 2016].

[64] Rampen J (2016) Airbnb hosts get first £1,000 tax free after Budget 2016 shake up. *Mirror,* 16 de marzo. Disponible en http://www.mirror.co.uk/money/airbnb-hosts-first-1000-tax-7568083 [accedido el 17 de agosto de 2016].

Sección 6

LA CANASTA DE DESARROLLO

La canasta de desarrollo

La tecnología es el principal motor para el cambio social. Siempre ha sido así (con la rueda, las herramientas agrícolas, la imprenta, el telégrafo, etc.). Se espera que los avances tecnológicos mejoren la sociedad. El pensamiento actual sobre el desarrollo y la tecnología se remonta al periodo de la ilustración y al crecimiento de la ciencia y la tecnología, del siglo XVI al XX. El núcleo de este pensamiento yace en el vínculo entre la tecnología y el progreso, así como también en la idea de que la tecnología puede resolver la mayoría de los problemas sociales; en su forma más simple, la tecnología debería provocar mayor desarrollo.

La tecnología también moldeó la agenda de desarrollo de la ONU, que fue promovida por primera vez después de la Segunda Guerra Mundial, en una maniobra para apoyar el desarrollo de los nuevos estados independientes, antiguas colonias. Si bien la tecnología contribuyó en la reducción de la pobreza y la mejora del bienestar de muchas personas, también enfrentó algunas limitaciones. Los desarrollos sociales y económicos son mucho más complejos que los tecnológicos. Exigen, por ejemplo, el desarrollo de la educación y la capacidad para empoderar a los individuos con el objetivo de que puedan hacer uso de nuevas tecnologías, así como también requieren de políticas e instituciones que reflejen tanto las culturas locales como la necesidad de adaptarse a los desarrollos modernos. Además, los ajustes sociales precisan tiempo, ya que la sociedad cambia un paso más lento que lo que la technologá se desarrolla.

El comunismo y el fracaso del desarrollo tecnológico

La mayor derrota histórica del desarrollo regido por la tecnología fue el fracaso del comunismo a finales del siglo XX. La ciencia y la tecnología eran las áreas priorizadas en la Unión Soviética y los países del este. A pesar de un comienzo tardío y recursos limitados, la Unión Soviética consiguió los mismos logros que los del mundo occidental en muchas áreas del desarrollo científico y tecnológico. Particularmente, hizo un buen trabajo con respecto a las tecnologías satelitales y militares. Sin embargo, la tecnología no fue suficiente para abordar los problemas socioeconómicos, por lo que el sistema colapsó. Muchas son las razones de este colapso, incluidas las ideológicas y estructurales; no obstante, una de las razones que todavía no está lo suficientemente investigada es la fuerte dependencia de las soluciones tecnológicas y de la tecno-ingeniería.

La era digital ha subrayado el poder habilitante de la tecnología. Existen numerosos ejemplos de cómo la Internet ha habilitado a muchos, desde el nivel individual hasta el mundial. Aun así, el vínculo entre el progreso tecnológico y el social no es automático, como explican numerosos estudios e informes.[1] Esta sección abordará la compleja interacción entre la tecnología y la sociedad. Algunas de las preguntas subyacentes son:

- ¿La Internet reducirá o ensanchará la brecha existente entre el mundo desarrollado y el mundo en vías de desarrollo?
- ¿Cómo y cuándo podrán ser capaces las naciones en desarrollo de llegar a los niveles digitales de los países desarrollados industrialmente?

- ¿Cómo pueden la Internet y las tecnologías digitales permitir el desarrollo sostenible, en sus diversas dimensiones?

Esta sección aborda los principales asuntos del desarrollo *per se*. Sin embargo, el desarrollo se ubica en un plano horizontal en muchos de los debates de políticas digitales. Casi todos los asuntos de la gobernanza de Internet tienen un aspecto relacionado con el desarrollo, como se ilustra en los siguientes ejemplos:

- El acceso a Internet – el primer requisito previo para cerrar la brecha digital – depende mayoritariamente de la existencia de una infraestructura de telecomunicación.

- El modelo económico actual para el acceso a Internet continúa imponiendo una carga desproporcionada sobre los países en vías de desarrollo, quienes tienen que financiar el acceso a las redes troncales ubicadas en los países desarrollados.

- El comercio electrónico brinda a las compañías en los países en desarrollo oportunidades para acceder al mercado global, pero estas compañías primero deben contar con el acceso a Internet.

Tecnologías digitales y desarrollo: elaboración de políticas

Los temas de desarrollo digital se incluyeron en la agenda mundial durante el proceso de la CMSI a principios de los años 2000. La primera resolución de la Asamblea General de la ONU sobre la CMSI hizo hincapié en la «promoción del desarrollo, en particular con respecto al acceso y a la transferencia de la tecnología».[2] Así, el objetivo general de la cumbre era contribuir en la reducción de la brecha digital entre los países desarrollados y los que están en vías de desarrollo, y facilitar la implementación de los objetivos de desarrollo del milenio (MDG, por sus siglas en inglés). La Declaración y el Plan de Acción de Ginebra de la CMSI remarcaron que el desarrollo era una prioridad y lo vincularon a la Declaración del Milenio de la ONU[3] y su promoción del acceso de todos los países a la información, el conocimiento, y las tecnologías de la comunicación para el desarrollo. Gracias al vínculo con los MDG,[4] la CMSI estaba posicionada fuertemente en el contexto del desarrollo. La Agenda de Túnez para la Sociedad de la Información también hizo frente a los problemas relacionados con las TIC para el desarrollo. Gran parte del documento está dedicado a los mecanismos financieros para enfrentar los desafíos conexos. Más de diez años después, el documento final de la reunión de alto nivel de la Asamblea General de la ONU sobre la revisión general de la implementación de los resultados de la CMSI (documento de resultados de la CMSI+10) estableció un vínculo entre la CMSI y los ODS[5] en el artículo 5:

> *Reconocemos que la mayor conectividad, innovación y acceso a las tecnologías de la información y las comunicaciones ha desempeñado una función esencial a los efectos de facilitar los progresos en relación con los Objetivos de Desarrollo del Milenio, y solicitamos que exista una estrecha armonización entre el proceso de la Cumbre Mundial sobre la Sociedad de la Información y la Agenda 2030 para el Desarrollo Sostenible, resaltando la contribución intersectorial de la tecnología de la información y las comunicaciones a los Objetivos de Desarrollo Sostenible y la erradicación de la pobreza, y observando que el acceso a las tecnologías de la información y las comunicaciones se ha convertido también en un indicador de desarrollo y en una aspiración en y por sí misma.*[6]

Los ODS hacen una referencia directa a la Internet en el Objetivo 9.c., que es «aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020». Además, en el marco de los ODS, se estableció el Mecanismo de Facilitación de la Tecnología, que investiga cómo la ciencia, la tecnología, y la innovación pueden facilitar la consecución de los ODS.[7]

También se destacó la temática del desarrollo en el IGF, que comenzó con la primera reunión en Atenas (2006), hasta el último IGF en 2015, en el que el tema dominante fue «La Evolución de la Gobernanza de Internet: Fortaleciendo el Desarrollo Sostenible».

¿De qué manera afectan las TIC el desarrollo de la sociedad?

Tras la adopción de los ODS, han surgido muchas iniciativas para la investigación de estas preguntas y la exploración de maneras en las que las TIC puedan catalizar el desarrollo.

Dichas iniciativas incluyen el programa de las TIC para el Desarrollo de la UNCTAD;[8] la Línea de Acción-Matriz ODS de la CMSI, que resume las maneras en que las TIC pueden colaborar con los diferentes ODS;[9] y las ediciones 2015 y 2016 del Foro de la CMSI, que se centraron en trazar un vínculo entre los ODS y las soluciones que pueden brindar las TIC.[10] Finalmente, la CSTD encausó sus actividades intersesionales del 2015-2016 en el tema «Prospectiva para el desarrollo digital», en el que examinaron los potenciales efectos a largo plazo que tendrían las últimas aplicaciones digitales (incluidos la IoT, la educación en línea, la impresión 3D, la automatización digital, etc.) sobre la economía, la sociedad, y el medio ambiente. La Comisión hizo varias recomendaciones para los gobiernos, alentándolos a, entre otras cosas, promulgar las políticas adecuadas para apoyar el desarrollo de las tecnologías emergentes y aprovechar las oportunidades que se desprenden de ellas, y promover un entorno de habilitación para el desarrollo digital, con una especial atención en áreas tales como el capital humano, la infraestructura de las TIC y la complementaria, y los marcos jurídicos.

El Informe de Desarrollo Mundial 2016: Dividendos Digitales[11] del Banco Mundial incorporó un enfoque precavido al debate de la conexión entre las TIC y el desarrollo, cuestionando la visión simplista de que más tecnología significa más desarrollo. El informe enfoca la atención al hecho de que, si bien la Internet (y, en general, las tecnologías digitales) tienen el potencial de habilitar el crecimiento y el desarrollo, las desigualdades y las brechas continúan existiendo e incluso empeoran a nivel internacional y dentro de los países.

Las tecnologías digitales aportan beneficios a las personas (fácil acceso a la información, oportunidades de trabajo y de otras índoles), a las empresas (mayor productividad y comercio, mejor competitividad e innovación), y a los gobiernos (mejores servicios públicos y aumento en la interacción con los ciudadanos). Sin embargo, estos beneficios no se reparten de una manera suficientemente uniforme y rápida como para permitir un real crecimiento económico mundial. Para superar este reto, el informe del Banco Mundial recomienda dos caminos principales: el de cerrar la brecha digital, y el de promulgar políticas complementarias que permitan a los usuarios individuales, empresas, y el sector público tomar el máximo provecho de las tecnologías digitales. Dichas políticas (denominadas colectivamente como complementos análogos) cubrirían las regulaciones que

incentivan la competitividad del mercado, y darían a las compañías una razón para innovar continuamente. Estas políticas estarían centradas en la educación y los programas de capacitación en el área de la competencia digital, y en instituciones públicas más capaces y transparentes que empleen la tecnología de manera efectiva en los procesos de elaboración de políticas y en la prestación de servicios públicos. Además, incluso si se dieran todos estos elementos, el desafío clave es cómo y cuándo usarlos y combinarlos.

El informe ratifica la vieja creencia de que la tecnología nunca es neutral. La historia de la humanidad brinda muchos ejemplos en los que la tecnología empodera a algunas personas, grupos, o naciones, excluyendo al resto. La Internet no es la excepción en este sentido: desde el nivel individual hasta el mundial, las oportunidades digitales se aprovechan de maneras distintas, y ha ocurrido un cambio en la distribución de la riqueza y el poder.

En resumen, los efectos de las TIC en el desarrollo socioeconómico son complejos y varían ampliamente. No obstante, el creciente interés en las dimensiones sociales y económicas de las TIC nos brinda posibilidades para medir mejor y desenredar la red del impacto de las TIC en la sociedad, y para descifrar cómo utilizar al máximo las aplicaciones de las TIC para el desarrollo socioeconómico.

www.igbook.info/development

La brecha digital

La brecha digital se puede definir como un distanciamiento entre aquellos que tienen el acceso y las capacidades para usar las TIC/Internet, y aquellos que no, por razones técnicas, políticas, sociales, o económicas. La OCDE se refiere a la brecha digital como «la brecha entre personas, hogares, empresas y áreas geográficas en diferentes niveles socioeconómicos con respecto a sus oportunidades de acceder a las tecnologías de la información y de la comunicación (TIC) y a su uso de la Internet para una amplia gama de actividades».[12]

La brecha digital no es un fenómeno aislado. Refleja las grandes desigualdades socioeconómicas en la educación, el cuidado de la salud, el capital, el resguardo, el empleo, el agua potable, y los alimentos.

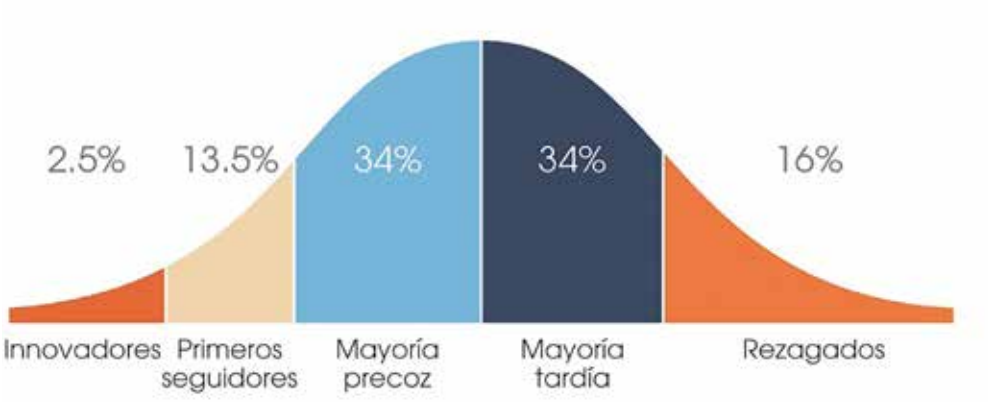

Figura 21. Curva de difusión de las innovaciones de Rogers

La curva de la difusión de las innovaciones de Rogers (Figura 21) ayuda a comprender la interacción esencial entre las posibilidades que ofrecen las herramientas tecnológicas, y las realidades de la percepción y la adopción de la tecnología. Clasifica a los adoptantes de las tecnologías en varias categorías desde innovadores hasta rezagados.

Se puede considerar que la curva de Rogers Curva también explica las brechas digitales que existen a diferentes niveles: dentro de los países y entre ellos, entre poblaciones rurales y urbanas, ancianos y jóvenes, hombres y mujeres, personas informadas y menos informadas, etc.

¿Se está ensanchando la brecha digital?

Los avances en las TIC/Internet dejan atrás a los países en vías de desarrollo mucho más rápidamente que cualquier otro tipo de avance (por ejemplo, en las técnicas agrícolas o médicas) y, ya que el mundo desarrollado cuenta con las herramientas necesarias para sacar buen provecho de estos avances tecnológicos, la brecha digital parece estar en constante y rápido crecimiento. Este punto de vista se encuentra desarrollado en varios documentos altamente respetados, como el de los Informes de Desarrollo Humano del Programa de las Naciones Unidas para el Desarrollo (UNDP), y los Informes sobre el Trabajo en el Mundo de la Organización Internacional del Trabajo (OIT).

Algunas opiniones opuestas señalan que las estadísticas sobre la brecha digital son engañosas, y que no solo que la brecha no está creciendo, sino que está disminuyendo.[13] Desde esta perspectiva, el foco tradicional sobre la cantidad de computadoras, el número de sitios web, o el ancho de banda disponible debería trasladarse hacia el amplio impacto de las TIC/Internet en las sociedades de los países en desarrollo. Algunos ejemplos frecuentemente citados son los éxitos digitales de Brasil, China, y la India.

De hecho, los criterios para evaluar los vacios en la brecha digital están cambiando y complejizándose para captar mejor las realidades del desarrollo. Las evaluaciones actuales toman en consideración aspectos como la disponibilidad de las TIC y su impacto en la sociedad. El FEM elaboró el Índice de Disponibilidad de Red (NRI, por sus siglas en inglés) como el nuevo enfoque en la medición de los niveles de Internet en los países de todo el mundo.[14] También brinda nuevas perspectivas sobre cómo se aborda la brecha digital.

Acceso universal

Además de la brecha digital, también se hace referencia frecuentemente al concepto de acceso universal, es decir, acceso a Internet para todos, en los debates sobre el desarrollo. Si bien debería ser la piedra angular de todas las políticas de desarrollo digital, continúan las diferencias en las percepciones o ideas sobre la naturaleza y el alcance del acceso universal. El debate sobre el acceso universal a nivel mundial permanece abierto, y depende principalmente de la preparación de los países desarrollados para invertir en la concreción de este objetivo, y también del entorno de políticas en los países en desarrollo. Aun así, la importancia del acceso universal recibe consenso en muchos documentos internacionales, como el documento final de la CMSI+10.

A diferencia del acceso universal a nivel mundial, en algunos países el acceso universal es un concepto económico y legal bien establecido. Los cimientos de las políticas de telecomunicaciones de EE. UU. es brindar a todos los ciudadanos el acceso a ellas. El resultado

es un sistema bien desarrollado de diferentes mecanismos políticos y financieros para subsidiar los costos de acceso en áreas remotas y regiones con elevados costos de conexión. El subsidio está financiado por las regiones con bajos costos de conexión, que suelen ser las grandes ciudades. La UE también dio pasos sólidos en relación con la obtención del acceso universal al promover políticas para asegurar que todos los ciudadanos tengan acceso a los servicios básicos de comunicación, incluida la conexión a Internet; también promulgó las regulaciones correspondientes.[15] Una propuesta para el Código Europeo de las Comunicaciones Electrónicas, presentada por la Comisión Europea en septiembre de 2016, planea redefinir la noción de servicio universal en el marco de la UE, quitando la atención a los servicios heredados (como las cabinas de teléfonos públicos) y concentrándola en la banda ancha.[16]

En los últimos tiempos, muchas compañías de Internet tomaron iniciativas para expandir el acceso a sus servicios. Intentan recopilar el enorme potencial económico de las regiones que todavía no están conectadas. Sus iniciativas se concentran en el método tradicional de construir el cableado o confiar en métodos menos tradicionales, como la diseminación de Internet mediante el uso de drones (Facebook) y globos (Google).

Consulte la Sección 2 para obtener más información sobre el debate acerca de la infraestructura de Internet y las soluciones innovadoras.

Estrategias para superar la brecha digital

Debido a que el acceso comprende distintas dimensiones – desde el acceso a la infraestructura hasta el acceso al contenido – tal y como lo explica el informe del CDH de la ONU,[17] superar la brecha digital a nivel mundial, regional y nacional representa un proceso complejo y a largo plazo, que requiere de una combinación de medidas, y políticas, así como también la participación de múltiples actores (los gobiernos, las organizaciones intergubernamentales, el sector privado, etc.):

El desarrollo de las infraestructuras de telecomunicación e Internet

El acceso a la infraestructura de Internet es uno de los principales desafíos para superar la brecha digital. Hay dos aspectos primordiales relacionados con el acceso a Internet en los países en vías de desarrollo. El primero es el acceso a las redes troncales internacionales de Internet. El segundo es la conectividad dentro de los países en vías de desarrollo.

El primero depende básicamente de la disponibilidad de cables de fibra óptica submarinos, que cumplen un papel protagónico en la conexión entre continentes. Debido a la geografía, pero también a los costos de empleo relativamente bajos, las principales redes troncales intercontinentales están sumergidas bajo los océanos. Actualmente, estos cables representan el medio por el que viaja más del 90% del tráfico mundial de Internet.

Consulte la Sección 2 para obtener más información sobre el cableado de la red troncal.

Además de los cables submarinos, surgieron planes para un cableado intercontinental terrestre estratégico. El proyecto chino Un Cinturón, Una Ruta, por ejemplo, examina el empleo de un cableado de fibra óptica terrestre para conectar Asia y Europa. Existen más cableados de enlace terrestre que se encuentran en su fase de planificación.

A largo plazo, el traslado hacia la comunicación de Internet por tierra podría causar un impacto de desarrollo de amplio alcance en los países euroasiáticos sin salida al mar. Se les podría ofrecer un acceso a Internet más fácil y menos costoso, en comparación con la situación actual en la que tienen que pagar elevados costos para acceder a Internet mediante el cableado submarino.

Otra solución hacia el acceso mejorado es la introducción de los IXP, que ayudan a mantener el tráfico local dentro del país. Sin los IXP, por ejemplo, el intercambio de correos electrónicos entre clientes de dos operadoras en un mismo país sería encaminado a través de la conexión internacional, y volvería al país. Los IXP son instalaciones técnicas mediantes las cuales diferentes PSI intercambian el tráfico de Internet mediante el *peering* (sin costo). Generalmente se instalan para mantener el tráfico de Internet en áreas más pequeñas (por ejemplo, en una ciudad, región, o país).

Aun así, muchos países en vías de desarrollo no cuentan con IXP, lo que significa que una gran parte del tráfico entre clientes de un mismo país se transfiere mediante otro país. Esto aumenta la cantidad de tráfico de datos internacionales de larga distancia del país en desarrollo y el costo de la prestación del servicio de Internet para ese país. Diferentes iniciativas tienen el objetivo de establecer IXP en países en vías de desarrollo.[18] Una que tuvo un éxito significativo fue la del Proyecto de Sistema de intercambio de Internet Africano (AXIS, en inglés) de la UA, que respaldó el establecimiento de IXP en África.

Otro desafío importante es la conectividad en los países en vías de desarrollo. Anteriormente, la mayoría de los usuarios de Internet estaban concentrados en las grandes ciudades. Las áreas rurales no tenían acceso a Internet. Esta situación comenzó a cambiar con el rápido desarrollo de la telefonía móvil y la comunicación inalámbrica.

La comunicación inalámbrica puede ser una alternativa viable para el desarrollo de infraestructuras de comunicaciones terrestres tradicionales, lo que a menudo es un reto. Esto implica colocar cables en grandes distancias a lo largo de muchos países asiáticos y africanos. En este contexto, las políticas sobre el espectro radioeléctrico son de extrema importancia para garantizar la disponibilidad del espectro y un uso eficiente de este. En este sentido, se podría vencer el problema de la última milla o el bucle local, uno de los obstáculos más grandes para un desarrollo de Internet más rápido. Sin embargo, existen opiniones que aseguran que las tecnologías móviles no son una solución definitiva, sino una provisoria, cuando se trata de cubrir grandes áreas que carecen de conectividad. Se sostiene que el espectro radioeléctrico tiene limitaciones físicas, por ejemplo, con respecto a la cantidad de dispositivos que pueden estar conectados a las redes inalámbricas.[19]

Tradicionalmente, el aspecto infraestructural de la brecha digital fue el foco de atención de la UIT mediante el UIT-D.

¿Quién debería cubrir los gastos del enlace entre los países desarrollados y los que están en vías de desarrollo?

Cuando un usuario final en África envía un correo electrónico a otro en Europa, EE. UU., o China, el PSI africano corre con los gastos de la conectividad internacional desde África a las principales redes troncales ubicadas en los centros de Internet más importantes en Europa, América del Norte, y Asia. Por otro lado, cuando un usuario final europeo envía un correo electrónico a África, sigue siendo el PSI africano quien cubre los gastos de conectividad internacional, por lo que, a fin de cuentas, el usuario final africano se lleva la peor parte, ya que debe pagar tarifas de suscripción más altas que cubren el flujo del tráfico digital en

ambas direcciones. Esto sucede porque los PSI de los países en desarrollo tienen dificultades para establecer acuerdo de *peering* de costo compartido con los grandes proveedores internacionales, a causa de contar con una base de clientes más pequeña. Estos PSI terminan funcionando como revendedores, ya que ellos compran la conectividad a proveedores internacionales, y la revenden a sus clientes nacionales, lo que resulta en precios elevados.[20]

El principal argumento en los debates sobre los cambios en el sistema actual de tarifas de Internet usa la analogía del sistema de pago del teléfono, que comparte los costos y las ganancias entre los puntos extremos de la comunicación. Sin embargo, Geoff Huston, director científico en APNIC, afirma que esta analogía no es sostenible.[21] En el sistema de telefonía, solamente un producto claramente identificable – una llamada telefónica que establece una conversación humana entre dos aparatos telefónicos – tiene precio. La Internet no cuenta con un único producto equivalente; tiene paquetes, que toman distintas rutas a través de la red. Esta diferencia fundamental hace que la analogía del teléfono no sea la adecuada. También es la razón principal por la cual el modelo de pago del servicio telefónico no se puede aplicar a Internet.

La UIT dio inicio a debates sobre las posibles mejoras por realizar en el sistema actual para el pago de los costos de Internet, con la intención de llegar a una distribución más equilibrada de costos. En 2008, se estableció la Recomendación D. 50 de la UIT, que incluyó recomendaciones para los acuerdos comerciales sobre las conexiones a Internet internacionales que tendrían en cuenta la necesidad de compensar los valores de elementos como el flujo del tráfico, el número de rutas, los costos de transmisión internacional, etc. entre las partes. Sin embargo, debido a la oposición de los países desarrollados y de las operadoras de telecomunicaciones, la recomendación quedó prácticamente sin efecto. Una de las limitaciones en la negociación de este problema entre los gobiernos es que la mayoría de los acuerdos de conexión se celebran entre operadoras de telecomunicaciones privadas, y casi siempre son confidenciales. Esto llevó a que la UIT adopte, en 2013, un Suplemento a la Recomendación D.50, que puso énfasis en las modalidades alternativas para la reducción de los costos de conectividad de Internet internacional, como los IXP, la instalación del cableado submarino, y el desarrollo de contenido local.[22]

Apoyo financiero

Durante el proceso de la CMSI, se reconoció la importancia del apoyo financiero para cerrar la brecha digital. Una idea que se propuso en la CMSI fue establecer una Fundación Solidaria Digital administrada por la ONU para ayudar a que los países con una desventaja tecnológica construyan infraestructuras de telecomunicaciones. Si bien se inauguró el Fondo mundial de Solidaridad Digital de manera oficial en marzo de 2005, no obtuvo un amplio respaldo por parte de los países desarrollados, que favorecieron a la inversión directa en lugar del establecimiento de un fondo centralizado para el desarrollo.

Los países en vías de desarrollo reciben apoyo financiero por medio de varios canales, como las agencias de desarrollo bilaterales o multilaterales, como el PUND o el Banco Mundial, así como también de iniciativas y bancos regionales para el desarrollo. La UIT inauguró un Fondo de Desarrollo de las TIC, una iniciativa de financiación inicial para contribuir en el fomento del desarrollo sostenible mediante la implementación de proyectos TIC relacionados con el desarrollo a nivel nacional, regional, y mundial. Más adelante, en junio de 2015, durante la Tercera Conferencia Internacional sobre la Financiación para el Desarrollo, se adoptó la Agenda de Acción de Addis Abeba, respaldada por la Asamblea General de la ONU. Esta agenda brinda un marco mundial para la financiación para el desarrollo sustentable, pasando por todos los ODS, y, como tal, podría incentivar aun más

el apoyo financiero para los países, con el objetivo de cerrar varias dimensiones de la brecha digital.[23]

Gracias a la liberalización del mercado de las telecomunicaciones, se vio aumentada la tendencia de desarrollar infraestructuras de telecomunicaciones mediante inversiones extranjeras directas. Dado que los mercados de telecomunicaciones de los países desarrollados están sobresaturados, muchas compañías de telecomunicaciones internacionales piensan que los mercados de los países en desarrollo son el camino para su futuro crecimiento.

Habilidades y competencias para el acceso efectivo

La habilidad básica de poder conectarse a Internet es un requisito previo para el acceso. Aun así, algunos creen que la definición de acceso es significativamente más amplia, y que debería tenerse en cuenta también la calidad de ese acceso. En este sentido, el documento final de la CMSI+10 suplicó que existiera «una evolución de la comprensión de lo que representa el acceso, haciendo foco en la calidad de ese acceso. [...] la velocidad, estabilidad, asequibilidad, idioma, contenido local y accesibilidad para las personas con discapacidades son, ahora, elementos de calidad».

La existencia de la infraestructura de las comunicaciones es inútil a menos que las personas cuenten con los medios (dispositivos) y el conocimiento (competencia de las TIC) para acceder y beneficiarse a través de Internet. Todavía son limitadas las contribuciones de los países en vías de desarrollo, en particular los de África, al conocimiento mundial en línea. La brecha entre el mundo desarrollado y el que está en vías de desarrollo se hace notar más en el área de la contribución de conocimiento que, por ejemplo, en el acceso a Internet. Por ejemplo, Hong Kong (RAE de China) proporciona más contenido a Wikipedia que la totalidad de África, aunque esta última cuenta con una cantidad de usuarios 50 veces mayor.[24]

Muchas iniciativas y organizaciones intentaron desarrollar habilidades y así abordar los aspectos socioculturales de la brecha digital. Por ejemplo, las iniciativas y organizaciones internacionales como *One Laptop per Child, Close the Gap, Computer Aid International* tienen como objetivo brindarles un equipamiento renovado y de bajo costo a las comunidades desfavorecidas en los países en desarrollo. También comenzaron iniciativas locales para brindar dispositivos asequibles. Singapur, por ejemplo, tiene un programa por el cual los estudiantes y las personas con discapacidad pertenecientes a familias de bajos ingresos tienen la oportunidad de adquirir una computadora a un precio que ellos pueden costear.[25]

Para los países en desarrollo, uno de los problemas principales es la fuga de cerebros – fenómeno por el cual los trabajadores más habilidosos se mudan de países en desarrollo a países desarrollados. Mediante la fuga de cerebros, los países en vías de desarrollo pierden a sus trabajadores mejor calificados, así como también sus inversiones en la capacitación y educación para ellos.

Es probable que este fenómeno continúe, dados los esquemas de empleo y migración que se introdujeron en EE. UU. y otros países desarrollados en miras de atraer a profesionales calificados, principalmente con formación en las TIC.

Por otro lado, un desarrollo que puede terminar o, en algunos casos, revertir la fuga de cerebros, es el incremento de la tercerización de las tareas TIC hacia los países en desarrollo. El ejemplo más exitoso es el desarrollo de los centros industriales de *software* en la India, como Bangalore y Hyderabad.

Aspectos de políticas y aspectos institucionales

Los asuntos de las políticas de telecomunicaciones están estrechamente unidos a la superación de la brecha digital en muchos aspectos:

- Ni los inversores privados ni los donantes públicos (cada vez menos) están dispuestos a invertir en países que no tengan un entorno institucional y jurídico adecuado para el desarrollo de Internet.

- El desarrollo de los sectores de las TIC nacionales depende de la creación de los marcos normativos necesarios.

- Las políticas de telecomunicaciones deberían facilitar el establecimiento de un mercado de telecomunicaciones eficiente mediante una mayor competencia, precios más bajos, y un rango más amplio de servicios prestados.

La creación de un entorno habilitante es una tarea exigente, que comprende la gradual desmonopolización del mercado de telecomunicaciones; la introducción de leyes relacionadas con Internet (que abarquen el derecho de autor, la privacidad, el comercio electrónico); y la disponibilidad del acceso a Internet para todos, sin restricciones políticas, religiosas, o de cualquier otra índole.

Uno de los primeros pasos es establecer autoridades regulatorias independientes y profesionales en lo que respecta a las telecomunicaciones. La experiencia de los países desarrollados demuestra que las estrategias normativas sólidas son el requisito *sine qua non* para el rápido crecimiento de la infraestructura de telecomunicaciones. Los países en vías de desarrollo han comenzado a adoptar este enfoque, pero algunos de ellos todavía se enfrentan a problemas con autoridades reguladoras generalmente débiles, carentes de independencia, o que son parte de un sistema en el que las operadoras de telecomunicaciones estatales influyen en el proceso normativo y político.

Otro desafío importante ha sido la liberalización del mercado de las telecomunicaciones. Usualmente se toma como ejemplo a la India y a Brasil, países en vías de desarrollo en los que la liberalización facilitó el rápido crecimiento de Internet y el sector de las TIC, y benefició a la economía en general. Algunos otros países, en particular los menos desarrollados, han descubierto que la liberalización del mercado de las telecomunicaciones es un enorme reto. Con la pérdida de los monopolios de la telecomunicación, los gobiernos de esos países perdieron una importante fuente de ingresos presupuestarios. Los bajos presupuestos afectaron a todos los demás sectores de la vida social y económica.

En algunos casos, además de que perdieron las ganancias de las telecomunicaciones, estos países no consiguieron beneficiarse a partir de la liberalización mediante los costos reducidos y los mejores servicios de telecomunicaciones. Esto se dio principalmente porque la privatización de estas compañías no fue reemplazada por la creación de mercados efectivos y la competencia. Estas prácticas hicieron que el Banco Mundial pusiera de relieve que los países deberían dar paso a grandes segmentos del mercado para la competencia antes o al mismo tiempo que la privatización de las operadoras estatales; de esta manera, reducirían los costos mucho más rápidamente que los países que llevan a cabo la privatización, y mucho tiempo después introducen a la competencia.

www.igbook.info/digitaldivide

Desarrollo de capacidades

La efectividad y legitimidad de la gobernanza de Internet depende de la capacidad de las naciones, organizaciones, e individuos que participan fuertemente en el proceso de políticas de la gobernanza de Internet. Las capacidades hacen referencia a las habilidades para «definir y resolver problemas, tomar decisiones fundadas, ordenar las prioridades, planificar el futuro, e implementar programas y proyectos para sostenerlos».[26]

Acerca del desarrollo de las capacidades

Aunque hay consenso sobre la importancia del desarrollo de las capacidades, no hay mucha comprensión sobre lo que incluye. Además, el término «desarrollo de las capacidades» generalmente se utiliza como una expresión en boga. En las negociaciones diplomáticas, el desarrollo de las capacidades es, por lo general, utilizado como mínimo común denominador cuando no hay consenso general en otros aspectos de las negociaciones.

Típicamente, el desarrollo de las capacidades se entiende como una capacitación. La interpretación del término se remonta a la década de 1950 y 1960, cuando la capacitación estaba en la cresta de la ola de los programas de asistencia técnica que ofrecían los países desarrollados a los que estaban en vías de desarrollo. Luego, en la década de 1970, el concepto de cooperación técnica comenzó a significar más que la simple transferencia de habilidades y conocimiento, y se encaminó hacia la contextualización dentro de las políticas y prioridades nacionales. Más recientemente (en la década de 1990), el desarrollo de las capacidades se concentró en el empoderamiento y fortalecimiento de las capacidades endógenas de los países en desarrollo.

Desarrollo de las capacidades o construcción de las capacidades

El desarrollo y la construcción de las capacidades son dos términos que se escuchan frecuentemente en los debates sobre el desarrollo. El primero hace referencia a las capacidades y habilidades endógenas presentes en todos los países, mientras que el segundo se utiliza en relación con el proceso de empezar desde cero y construir algo que previamente no existía. El término «construcción de las capacidades» se utiliza de una manera más generalizada en el lenguaje actual sobre el desarrollo.

El desarrollo de las capacidades podría definirse haciendo referencia a los tipos de capacidades y a los niveles en los que se desarrollan.

Los tipos de capacidades incluyen:

- Las capacidades duras, que incluyen el conocimiento técnico y especializado, y el *know-how* (por ejemplo, conocimiento sobre ingeniería).
- Las capacidades blandas, que se dividen generalmente en dos subgrupos:
    - Capacidades operativas: comunicación intercultural, liderazgo, cultura y valores organizacionales, capacidad para resolver problemas.

- Capacidades adaptativas: habilidad de analizar y adaptarse, preparación y gestión ante los cambios, confianza.

Las capacidades duras generalmente se consideran técnicas y visibles, mientras que las blandas son más racionales e invisibles.

Los varios niveles en los que se desarrollan y necesitan estas capacidades se pueden ver mediante el modelo mariposa del desarrollo de las capacidades (Figura 22, basado en la metodología utilizada por la Agencia Suiza para el Desarrollo y la Cooperación).[27]

Figura 22. Mariposa del desarrollo de las capacidades

Desarrollo de las capacidades en la gobernanza de Internet y las políticas digitales

La necesidad de contar con un desarrollo de las capacidades es una característica subyacente en la gobernanza de Internet desde el documento final de la CMSI 2003-2005, que resaltó que el desarrollo de las capacidades era una prioridad para los países en desarrollo. De la misma manera, el documento final de la CMSI+10 de 2015 exige una mayor inversión en el desarrollo de las capacidades.

Dada la naturaleza novedosa de la gobernanza de Internet, el foco principal ha estado en la capacitación personal y la inmersión en las políticas.

Muchas organizaciones, incluidas la UIT, DiploFoundation, y la Geneva Internet Platform (GIP),[28] junto con APC, la Internet Society, y ICANN, cuentan con programas específicos de desarrollo de las capacidades. Muchas escuelas de verano regionales sobre la gobernanza de Internet también ayudan al fortalecimiento de las capacidades, particularmente

para los países en vías de desarrollo. Muchos de los programas disponibles se enfocan en la infraestructura de las telecomunicaciones, los estándares técnicos, la ciberseguridad, el correo no deseado, la regulación de las TIC, la libertad de expresión, el comercio electrónico, el derecho laboral, el acceso, y la superación de la brecha digital.

Cientos de personas se instruyen en la gobernanza de Internet y las políticas digitales. La transición hacia una fase más experimentada requeriría una atención más concentrada en el desarrollo organizacional, asegurando la participación sostenida en los procesos políticos. Esto implica desarrollar las capacidades organizacionales de los gobiernos, la sociedad civil, las organizaciones comerciales, y el sector académico en los países en desarrollo. El desarrollo de capacidades organizacionales y a nivel de sistema está cobrando mayor relevancia en el abordaje de asuntos como la ciberseguridad.

La investigación sobre el desarrollo de las capacidades en general y la experiencia del campo de la gobernanza de Internet desembocaron en los siguientes asuntos destacados:

- Si bien la Internet es un servicio mundial, sus políticas, por lo general, son bastante locales. Se moldean en base a las especificidades culturales y sociales locales (por ejemplo, sensibilidad cultural hacia ciertos contenidos, relevancia de la protección de la privacidad). Por lo tanto, el desarrollo de las capacidades debería seguir la dinámica local, tomando en consideración las condiciones políticas, sociales, culturales y de otra índole del lugar en el desarrollo y la implementación de los programas y actividades para el desarrollo de las capacidades.

- La urgencia del desarrollo de las capacidades se podría abordar mediante las capacitaciones «justo a tiempo» como parte de los procesos de políticas. DiploFoundation y la GIP utilizan algunos elementos de este enfoque en la capacitación «justo a tiempo» para diplomáticos. ICANN hace lo propio en su Programa de Becas,[29] al igual que la Internet Society, en su Programa de Embajadores del IGF.[30]

- La creciente necesidad de contar con capacidades en el campo de las políticas digitales debe abordarse a un nivel más sistemático, mediante la inclusión de la gobernanza de Internet y temas conexos en los programas de estudios académicos de posgrado.

- El empoderamiento genuino y sostenible se puede conseguir a través del desarrollo holístico de capacidades a nivel personal, organizacional, sistémico, y de red, como se puede ver en el modelo mariposa del desarrollo de las capacidades (Figura 22).

www.igbook.info/capacitydevelopment

NOTAS FINALES

[1] Dos de esos estudios son: Banco Mundial (2016) Informe de Desarrollo Mundial 2016: Dividendos digitales. Disponible en http://www.worldbank.org/en/publication/wdr2016 [accedido el 29 de octubre de 2016], y la Alianza para una Internet Asequible (2016) Informe de asequibilidad 2015-2016. Disponible en http://a4ai.org/affordability-report/report/2015/ [accedido el 5 de noviembre de 2016].

[2] Asamblea General de las Naciones Unidas (2002) Resolución A/56/183. Cumbre Mundial sobre la Sociedad de la Información. Disponible en http://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002.pdf [accedido el 27 de octubre de 2016].

[3] Asamblea General de las Naciones Unidas (2000) Resolución A/55/L.2. Declaración del Milenio de las Naciones Unidas. Disponible en http://www.un.org/millennium/declaration/ares552e.htm [accedido el 27 de octubre de 2016].

[4] Naciones Unidas (sin fecha) Objetivos de Desarrollo del Milenio. Disponible en http://www.un.org/millenniumgoals/ [accedido el 27 de octubre de 2016].

[5] Asamblea General de las Naciones Unidas (2015) Resolución A/70/1. Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible. Disponible en http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E [accedido el 27 de octubre de 2016].

[6] Asamblea General de las Naciones Unidas (2015) Resolución A/70/125. Documento final de la reunión de alto nivel de la Asamblea General sobre la revisión general de la implementación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información. Disponible en http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf [accedido el 27 de octubre de 2016].

[7] Para obtener más información sobre la conexión entre los ODS e Internet, consulte: *GIP Digital Watch* observatory (sin fecha) Objetivos de Desarrollo Sostenible y la Internet. Disponible en http://digitalwatch.giplatform.org/processes/sustainable-development-goals [accedido el 11 de agosto de 2016].

[8] UNCTAD (sin fecha) Tecnología de la Información y la Comunicación para el Desarrollo. Disponible en http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D.aspx [accedido el 27 de octubre de 2016].

[9] Foro de la CMSI (2015) Matriz CMSI-ODS: Objetivos de Desarrollo Sostenible y Líneas de Acción de la CMSI. Ginebra: Unión Internacional de las Telecomunicaciones. Disponible en https://www.itu.int/net4/wsis/sdg/Content/wsis-sdg_matrix_document.pdf [accedido el 27 de octubre de 2016].

[10] Para obtener más detalles sobre los debates en las ediciones 2015 y 2016 del Foro de la CMSI, consulte: *GIP Digital Watch* observatory (sin fecha) Foro de la CMSI de 2015. Disponible en https://digitalwatch.giplatform.org/events/wsis-forum-2015 [accedido el 28 de octubre de 2016]; y *GIP Digital Watch* observatory (sin fecha) Foro de la CMSI 2016. Disponible en http://digitalwatch.giplatform.org/events/wsis-forum-2016 [accedido el 28 de octubre de 2016].

[11] Banco Mundial (2016) Informe de Desarrollo Mundial 2016: Dividendos digitales. Disponible en http://www.worldbank.org/en/publication/wdr2016 [accedido el 29 de octubre de 2016].

[12] OCDE (2001) Understanding the Digital Divide. p. 5. Disponible en http://www.oecd.org/Internet/ieconomy/1888451.pdf [accedido el 27 de octubre de 2016].

[13] Internet World Stats (2016) Digital Divide Gap is Getting Smaller. Disponible en http://Internetworldstats.com/wp/digital-divide-gap-is-getting-smaller/ [accedido el 30 de octubre de 2016].

[14] FEM (2016) Reporte Mundial de Tecnologías de la Información. Disponible en https://www.weforum.org/reports/the-global-information-technology-report-2016 [accedido el 27 de octubre de 2016].

[15] Unión Europea (2014) Servicio Universal. Disponible en http://ec.europa.eu/digital-agenda/en/universal-service [accedido el 27 de octubre de 2016].

[16] Comisión Europea (2016) Propuesta de Directiva del Parlamento Europeo y el Consejo por la que se establece el Código Europeo de las Comunicaciones Electrónicas. Disponible en https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code [accedido el 28 de octubre de 2016].

[17] Naciones Unidas (2011) Informe del Relator Especial para la promoción y la protección del derecho a la libertad de expresión, Frank La Rue. Disponible en http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf [accedido el 28 de octubre de 2016]. Para leer un debate sobre el informe de la ONU, consulte: Wagner A (2012) Is Internet access a human right? *The Guardian*, 11 de enero. Disponible en https://www.theguardian.com/law/2012/jan/11/is-internet-access-a-human-right [accedido el 28 de octubre de 2016].

[18] Internet Society (2012) Promoción del uso de los Puntos de Intercambio de Tráfico (IXP): Una guía sobre cuestiones técnicas, de políticas y de gestión. Disponible en https://www.Internetsociety.org/sites/default/files/Promoting%20the%20use%20of%20IXPs.pdf [accedido el 5 de noviembre de 2016].

[19] Diálogo del Sudeste Europeo sobre la Gobernanza de Internet (2016) SEEDIG's contribution to the IGF 2016 Inter-sessional Programme on Policy Options for Connecting and Enabling the Next Billion – Phase II. Disponible en http://www.seedig.net/wp-content/uploads/2016/09/SEEDIG-contribution-to-IGF-CENB-II.pdf [accedido el 28 de octubre de 2016].

[20] Berkman Center for Internet & Society, Harvard Law School (2003) BOLD 2003: Development and the Internet, Part 4: Solutions in the Architecture. Disponible en http://cyber.law.harvard.edu/bold/devel03/modules/modIC.html [accedido el 28 de octubre de 2016].

[21] Huston G (2005) Where's the Money? Internet Interconnection and Financial Settlement. *The ISP Column*, enero de 2005, Internet Society, pp. 7–9. Disponible en http://www.potaroo.net/ispcol/2005-01/interconn.pdf [accedido el 27 de octubre de 2016].

[22] La Recomendación UIT-T D. 50, y sus suplementos, están disponibles en http://www.itu.int/rec/T-REC-D.50/e [accedido el 11 de agosto de 2016].

[23] Naciones Unidas (2015) Agenda de Acción de Addis Abeba de la Tercera Conferencia Internacional sobre la Financiación para el Desarrollo. Disponible en http://www.un.org/esa/ffd/publications/aaaa-outcome.html [accedido el 28 de octubre de 2016].

[24] Banco Mundial (2016) Informe de Desarrollo Mundial 2016: Dividendos digitales. Disponible en http://www.worldbank.org/en/publication/wdr2016 [accedido el 29 de octubre de 2016].

[25] Autoridad de Desarrollo de Infocomunicaciones de Singapur (sin fecha) NEU PC Plus Programme. Disponible en https://www.imda.gov.sg/community/consumer-education/digital-inclusion/neu-pc-plus-programme [accedido el 15 de agosto de 2016].

[26] Agencia Suiza para el Desarrollo y la Cooperación (2006) Glossary Knowledge Management and Capacity Development. Disponible en https://www.eda.admin.ch/dam/deza/en/documents/publikationen/glossar/157990-glossar-wissensmanagement_EN.pdf [accedido el 5 de noviembre de 2016].

[27] Agencia Suiza para el Desarrollo y la Cooperación (2006) Capacity Development in SDC. Disponible en https://www.eda.admin.ch/content/dam/deza/en/documents/die-deza/strategie/202114-capacity-development-sdc_EN.pdf [accedido el 5 de noviembre de 2016].

[28] Las actividades para el desarrollo de las capacidades de Diplo incluyen el Programa de Construcción de Capacidades de la Gobernanza de Internet; cursos en línea sobre gobernanza de Internet, ciberseguridad, e infraestructura técnica; maestrías en diplomacia contemporánea con especialización en gobernanza de Internet. Más recientemente, al operar la GIP, Diplo brinda la capacitación «justo a tiempo» para misiones permanentes.

[29] ICANN (sin fecha) Programa de Becas ICANN. Disponible en https://www.icann.org/fellowshipprogram [accedido el 7 de noviembre de 2016].

[30] Internet Society (sin fecha) Programa de Embajadores del IGF. Disponible en http://www.internetsociety.org/what-we-do/education-and-leadership-programmes/next-generation-leaders/igf-ambassadors-programme [accedido el 7 de noviembre de 2016].

Sección 7

LA CANASTA SOCIOCULTURAL

La canasta sociocultural

La Internet ha provocado un gran impacto en la estructura social y cultural de la sociedad moderna. Resulta difícil identificar un segmento de nuestra vida social que no esté afectada por La Internet. Ella introduce nuevos patrones de comunicación social, derriba barreras lingüísticas, y crea nuevas formas de expresión creativa. Estos son solo algunos de sus efectos. Hoy en día, la Internet es un fenómeno tan social como tecnológico.

Políticas de contenido

Uno de los principales asuntos socioculturales es el de las políticas de contenido, que es a menudo abordado desde las perspectivas de: las políticas de los gobiernos (medidas de control de contenido impuestas por varias consideraciones, y que varían desde la seguridad nacional, la ética, y el orden púbico, hasta formas de censura por razones políticas), los derechos humanos (el impacto de las políticas de contenido sobre la libertad de expresión y el derecho a la comunicación), y la tecnología (herramientas para el control del contenido). Los debates generalmente se centran en tres grupos de contenidos.

- Contenido que cuenta con consenso global para su control. En este grupo se incluye el contenido relacionado con el abuso sexual infantil, la justificación del genocidio, y la incitación a actos terroristas o a la organización de estos.

- Contenido que es sensible para ciertos países, regiones, o grupos étnicos debido a sus valores religiosos y culturales en particular. La comunicación en línea globalizada presenta desafíos para los valores locales, culturales, y religiosos de muchas sociedades. Gran parte del control de contenido en países del Medio Oriente y de Asia, por ejemplo, se justifica oficialmente por la protección de valores culturales específicos. Esto a menudo significa que el acceso a sitios web de pornografía o de juegos de apuestas está bloqueado.

- Censura política en la Internet, por lo general para acallar la disidencia política bajo la afirmación de protección de la seguridad y estabilidad nacional.[1]

Cómo se gestionan las políticas de contenido

Un menú a la carta para las políticas de contenido contiene las siguientes opciones legales y técnicas, que se usan en diferentes combinaciones.

Filtrado de contenido por parte del gobierno

Los gobiernos que filtran el acceso a contenido usualmente crean un Índice de Internet de sitios web bloqueados para el acceso de los ciudadanos. En términos más técnicos, el filtrado utiliza principalmente un bloqueo IP basado en el enrutador, servidores proxy, y el redireccionamiento DNS. El filtrado de contenido se lleva a cabo en muchos países. Además de los países que usualmente están asociados a tales prácticas, como China, Arabia

Saudita, y Singapur, también otros países están implementando medidas de filtrado cada vez con mayor frecuencia.[2]

Sistemas de filtrado y tasación privada

Frente a potenciales riesgos de desintegración de la Internet a causa de la creación de varias barreras nacionales (sistemas de filtrado), el W3C y otras instituciones afines llevaron a cabo maniobras proactivas para proponer la implementación de sistemas de filtrado y tasación controlada por los usuarios. En estos sistemas, pueden implementarse mecanismos de filtrado por *software* en las computadoras personales o a nivel del servidor que controla el acceso a Internet.

Esta posibilidad le permite a los usuarios de diferentes países y culturas implementar sus propios sistemas de filtrado, obviando la necesidad de una intervención nacional que podría provocar la fragmentación de la Internet en bloques nacional o culturalmente filtrados. Lo que aún está por verse es si los gobiernos les confiarán a sus ciudadanos la posibilidad de llevar a cabo los filtrados que los estados consideren necesarios. Es probable que esto se trate de un recurso adicional personalizado para los usuarios, en lugar del reemplazo del filtrado sistemático por parte del gobierno.

El control de contenido por parte del gobierno por motivos de religión en determinados países es un tema bastante conocido, pero el filtrado por motivos religiosos también podría llevarse a cabo y ser apoyado por ciertas organizaciones. Por ejemplo, en 1998, un paquete de *software* fue distribuido, según se dijo, por el movimiento de la Cienciología a sus miembros. Algunos críticos apodaron al *software* «Scieno sitter» y afirmaron que evitaba el acceso a sitios web críticos de la Cienciología.[3] Otros ejemplos podrían afectar a poblaciones enteras: por ejemplo, el lobby cristiano de Australia presionó al gobierno australiano para imponer un sistema de filtrado *opt-out* que bloquearía «contenido para adultos» en los hogares de Australia y también en dispositivos móviles.[4]

Filtrado de contenido basado en la región geográfica

Otra solución técnica relacionada con el contenido es el software de geolocalización, que filtra el acceso a un contenido web en particular de acuerdo con el origen geográfico o nacional de sus usuarios. El caso Yahoo! tuvo gran importancia en este sentido, ya que el grupo de expertos involucrados, incluido Vint Cerf, indicó que entre el 70% y el 90% de los casos, Yahoo! podía determinar si se accedía desde Francia a ciertas secciones de uno de sus sitios web que alojaba objetos de interés Nazi.[5] Esta evaluación contribuyó a que la corte tomara una decisión final en la que le solicitó a Yahoo! filtrar el acceso a la memorabilia Nazi desde Francia. A partir del caso de Yahoo! del 2000, la precisión de la geolocalización se ha incrementado aún más mediante el desarrollo de *software* de geolocalización altamente sofisticado.

Control de contenido por medio de motores de búsqueda

El puente que conecta al usuario final con el contenido web es, por lo general, un buscador. El filtrado de los resultados de búsqueda es, en consecuencia, también usado como herramienta para prevenir el acceso a determinado contenido. Dicho filtrado se implementa a menudo por parte de los buscadores para cumplir con las políticas gubernamentales. Un ejemplo importante es el de Google en China. En 2006, Google decidió lanzar una versión local de su motor de búsqueda (google.cn) que estaba destinado a cumplir con las políticas del gobierno de China en lo que respecta al filtrado de contenido en línea considerado objetable. En 2010, la compañía cambió su enfoque al redireccionar búsquedas llevadas a

cabo en Google.cn a sus servidores ubicados en Hong Kong (los cuales no contaban con el filtrado). Esto resultó en una tensa relación con el gobierno, el que, al final, decidió que Google debía cerrar sus operaciones en China.[6]

El filtrado de resultados de búsqueda no solo se implementa desde la esfera gubernamental; los intereses comerciales también pueden interferir, de una manera más o menos obvia o dominante. Los analistas han comenzado a cuestionar el rol de los buscadores en la mediación del acceso por parte del usuario a la información, y han comenzado a advertir también acerca del poder que pueden ejercer para influenciar los conocimientos y preferencias de los usuarios.[7] Este asunto está llamando la atención de los gobiernos cada vez más, quienes exigen una mayor transparencia en las prácticas de las compañías de Internet. A modo de ejemplo, en un discurso pronunciado en octubre de 2016, la canciller alemana Angela Merkel instó a las compañías de Internet a poner a disponibilidad del público la información relacionada con los algoritmos que utilizan en sus buscadores. Tal información, según Merkel, ayudaría a los usuarios a entender mejor cómo y sobre qué base se les presenta la información que reciben a través de los buscadores. La canciller concluyó: «Los algoritmos, cuando no son transparentes, pueden dar lugar a una distorsión de la percepción, que estrechan nuestra amplitud de la información».[8]

Desafío web 2.0: contenido generado por el usuario

Con el desarrollo de plataformas web 2.0 – blogs, foros, sitios web en donde se comparten documentos, y las redes sociales – , la diferencia entre el usuario y el creador ya no resulta muy clara. Los usuarios de Internet se han vuelto los creadores de grandes cantidades de contenido web, como las publicaciones en blogs, vídeos, y galerías de fotos. La identificación, el filtrado, y la clasificación de los sitios web como «inadecuados» representan una actividad compleja. Mientras que las técnicas de filtrado automático para textos son avanzadas, el reconocimiento, el filtrado, y la clasificación del contenido visual de manera automática todavía se encuentran en su fase de desarrollo.

Un enfoque que suelen tomar los gobiernos en sus intentos por abordar el tema del contenido generado por el usuario que ellos consideran objetable es el de bloquear por completo el acceso a plataformas como YouTube y Twitter en todo el país. Este enfoque maximalista, sin embargo, resulta en el bloqueo también de contenido no objetable, como el material educativo. Otra medida, aunque más extrema, es la de cortar por completo el acceso a Internet para dificultar la comunicación a través de plataformas de redes sociales (como sucedió, por ejemplo, durante los eventos de la Primavera Árabe).[9]

Debido a que el debate sobre qué se puede y qué no se puede publicar en línea ha madurado bastante, las propias plataformas de redes sociales han comenzado a formalizar sus políticas en las que indican dónde se ubica la línea que divide el contenido que debería ser tolerado del que no. Por ejemplo, la Declaración de Derechos y Responsabilidades de Facebook especifica: «Podemos remover cualquier contenido o información que publiques en Facebook si consideramos que infringe esta Declaración o nuestras políticas».[10] Sin embargo, la implementación de tales políticas a veces puede llevar a consecuencias no deseadas, en las que las plataformas eliminan contenido legítimo.

Control del contenido automatizado

A las compañías de redes sociales de Internet les resulta difícil identificar contenido ilegal de entre los millones de videos y aportes de contenido de sonido o de texto. Una posible solución para este desafío podría estar basada en el uso de mecanismos de IA. Un ejemplo

del potencial de la IA en este campo es *Conversation AI* – una herramienta desarrollada por Jigsaw, el *start-up* impulsado por Google, con el objetivo de detectar discursos del odio y otras formas de abuso y acoso verbal en línea.[11] A partir de octubre de 2016, el *software,* que depende de la poderosa tecnología de datos de Google, se encontrará en su fase de evaluación. Sin embargo, el hecho de confiar en que una máquina tome decisiones con respecto a qué constituye un discurso del odio abre varias preguntas, tales como si estos sistemas serán capaces de diferenciar entre discurso del odio, la ironía y el sarcasmo.

Instrumentos legales y de políticas en el control de contenido

El contenido, en forma de expresión escrita y verbal, siempre ha estado en el foco de atención de las políticas públicas. Las sociedades deciden cuándo se trata de contenido aceptable y cuándo no, basándose en consideraciones políticas, de seguridad, y religiosas. Las políticas van desde fomentar la libertad de expresión hasta imponer censura. La Internet ha entrado en este campo de políticas sensibles al simplificar como nunca antes la diseminación de información y contenido. Por lo tanto, nos enfrentamos a una situación paradójica caracterizada, por un lado, por un campo de políticas de contenido altamente regulado, y por el otro, por un vacío legal en lo que respecta a la aplicabilidad de las políticas de contenido tradicionales a la Internet.

Nivel nacional

El vacío legal en el campo de las políticas de contenido en línea provoca incertidumbre jurídica. La reglamentación nacional en este campo podría crear una situación legal más predecible, y asegurar una mejor protección de los derechos humanos como la libertad de expresión y la libertad de información. Además, las normas legales podrían reducir el alto nivel de discrecionalidad del que disfrutan los gobiernos con respecto a las políticas de contenido. El sector comercial, en particular los PSI y las compañías de Internet, podría también resultar beneficiado al evitar situaciones ambiguas al momento de decidir sobre cuestiones de políticas de contenido.

Debido a que la línea divisoria entre el control de contenido justificado y la cesura no está bien delimitada, y por lo tanto resulta difícil de incluir en la legislación, la tensión se está resolviendo en los tribunales cada vez con mayor frecuencia. Por ejemplo, varios medios de comunicación social fueron demandados en mayo de 2016 por permitir contenido racista y homofóbico en sus plataformas.[12] Además, tras los ataques en París en noviembre de 2015 y en Israel entre 2014 y 2016, se ha acusado a los medios de comunicación social de proporcionar una plataforma que los terroristas pueden utilizar «para comunicarse, reclutar miembros, planear y llevar a cabo ataques, e infundir miedo en sus enemigos»,[13] además de facilitar la difusión de la propaganda terrorista.[14]

Iniciativas internacionales

Frente a las amenazas terroristas y la sofisticación aumentada con la que los terroristas gestionan sus actividades y promueven sus ideologías en línea, algunos foros multilaterales han comenzado a analizar posibles maneras de limitar este contenido nocivo. Por ejemplo, los líderes del G7 concordaron en «mejorar los esfuerzos para contrarrestar las amenazas impuestas por grupos terroristas que explotan la Internet y los medios sociales con fines terroristas».[15]

Además, el Consejo de Seguridad de la ONU ha solicitado al Comité contra el Terrorismo proponer directrices y buenas prácticas para contrarrestar el uso de la Internet por parte

de terroristas para promover sus narrativas y reclutar más miembros.[16] Más concretamente, la UNODC publicó un informe acerca del uso de la Internet con fines terroristas.[17]

Consulte la Sección 3 para obtener más información acerca de cómo luchar contra la distribución de la propaganda terrorista y el contenido violento de grupos extremistas en línea.

A nivel regional, las principales iniciativas de regulación han surgido en países europeos con fuerte legislación en el campo del discurso del odio, incluidos también el antirracismo y el antisemitismo. Algunas instituciones regionales europeas han intentado imponer estas reglas en el ciberespacio. El principal instrumento legal que aborda el problema del contenido es el del CdE de 2003: el Protocolo adicional al Convenio sobre la Ciberdelincuencia,[18] sobre la penalización de actos de naturaleza racista o xenófoba llevados a cabo mediante sistemas informáticos. En un nivel más práctico, en 2012, la UE adoptó la Estrategia europea en favor de una Internet más adecuada para los niños. Con esta estrategia, se han implementado diferentes actividades y programas para crear consciencia, luchar contra el contenido ilegal, implementar el filtrado y la clasificación de contenido, trabajar con la sociedad civil en asuntos de seguridad de los niños en línea, y crear una base de datos de información acerca del uso que los niños le dan a la tecnología.[19]

La OSCE también tiene un rol activo en este campo. Desde 2003, ha organizado una serie de conferencias y reuniones con un enfoque particular sobre la libertad de expresión y los potenciales usos indebidos de la Internet (por ejemplo: la propaganda racista, xenófoba, y antisemita; y el contenido relacionado con el extremismo violento y la radicalización que lleva al terrorismo).

Los asuntos

El control del contenido y la libertad de expresión

A menudo se considera que el control del contenido causa una posible restricción en la libertad de expresión. Muchas sociedades en el mundo intentan abordar esta área sensible mediante la promoción de la libertad de expresión, mientras que permiten un control de contenido excepcional y públicamente justificado. Esto es de especial importancia en los EE.UU., en donde la Primera Enmienda garantiza una amplia libertad de expresión, e incluso el derecho a publicar material Nazi o contenido similar.

La libertad de expresión moldea en gran medida la posición de EE.UU. en el debate internacional sobre asuntos relacionados con el contenido en la Internet. Por ejemplo, si bien EE.UU. ha firmado el Convenio sobre la Ciberdelincuencia, no puede firmar el Protocolo Adicional a este convenio, que trata sobre el discurso del odio y el control de contenidos. El asunto sobre la libertad de expresión fue también mencionado en el contexto de la causa judicial de Yahoo!. En sus iniciativas internacionales, EE.UU. no traspasará la línea que podría poner en peligro la libertad de expresión, tal y como se estipula en la Primera Enmienda.

Ilegal fuera de línea – ilegal en línea

Como sucede con los derechos humanos, la opinión dominante es que las reglas del mundo fuera de línea aplican a la Internet cuando se trata de políticas de contenido.

Uno de los argumentos del enfoque cibernético sobre la regulación de Internet es que la cantidad (intensidad de la comunicación, número de mensajes) hace una diferencia en cuanto a la calidad. De esta manera, el problema del discurso del odio no se basa en que no se han promulgado leyes en su contra, sino que el contenido compartido y diseminado a través de la Internet lo encuadra dentro de un problema legal de diferente naturaleza. Más individuos están expuestos y resulta difícil hacer cumplir las reglas ya existentes. Por lo tanto, la diferencia que provoca la Internet se relaciona principalmente con los problemas de aplicación, no con las reglas en sí.

Consulte la Sección 4 para obtener más información acerca del enfoque del ciberderecho sobre la regulación de la Internet.

La efectividad del control de contenido

En los debates sobre políticas de Internet, uno de los argumentos clave es que la naturaleza descentralizada de Internet puede pasar por alto la censura. En los países que cuentan con un control de contenido gestionado por el gobierno, los usuarios con talentos técnicos han encontrado brechas en el sistema de control (por ejemplo: acceder a contenido filtrado a través de las VPN, o habilitar un contenido en una ubicación diferente de la que posee bloqueos para su acceso). Además, expertos han advertido acerca de que las medidas de filtrado pueden también tener consecuencias negativas en el nivel técnico. El bloqueo a nivel del DNS puede, por ejemplo, entrar en conflicto con la adopción de las DNSSEC, y podría también promover la fragmentación de Internet.[20]

Quiénes deberían ser los responsables de las políticas de contenido

Los principales actores en el área de control de contenido son los parlamentos y los gobiernos. Casi siempre, aplican principios básicos constitucionales en relación con qué tipo de contenido debe controlarse y de qué manera. Los PSI, como portales de Internet, son considerados responsables de la implementación del filtrado de contenido, ya sea de acuerdo con las disposiciones del gobierno o por autorregulación (al menos en lo que respecta a asuntos de amplio consenso, como la pornografía infantil). Algunos grupos de usuarios, como los padres, están a favor de la implementación de una política de contenido más eficiente para proteger a los niños. Varias iniciativas de tasación ayudan a los padres a encontrar contenido apto para menores. Versiones nuevas del *software* de navegación de Internet por lo general incluyen varias opciones de filtrado.

Las compañías de Internet (como Facebook, Google, y Twitter) se están convirtiendo en reguladoras de contenido *de facto*. Google, por ejemplo, ha tenido que decidir dentro de más de medio millón de solicitudes para eliminar enlaces de los resultados de búsquedas, basados en el derecho al olvido.

Consulte la Sección 4 para obtener más información acerca de los mecanismos de resolución de las disputas relacionadas con el contenido en línea, implementados por las compañías de Internet.

Estas compañías están cada vez más comprometidas en esfuerzos cooperativos con las autoridades públicas en su intento por combatir el contenido ilegal en línea. A modo de ilustración de esta tendencia, compañías tecnológicas en Silicon Valley han llevado a cabo

varias reuniones con las autoridades de EE.UU. a lo largo del 2016, en las que se debatió acerca de las oportunidades de cooperación en asuntos relacionados con el control del contenido en línea, específicamente en lo que respecta al contenido relacionado con el terrorismo.[21] En la UE, las compañías TI han trabajado conjuntamente con la Comisión Europea sobre la base de un código de conducta para los discursos del odio ilegales en línea, que incluye una serie de compromisos para evitar la diseminación de estos discursos en Europa.[22]

www.igbook.info/contentpolicy

Educación en línea

La Internet abrió nuevas posibilidades para la educación. Las iniciativas en línea y el aprendizaje electrónico utilizan a la Internet como el medio para la facilitación de cursos a participantes de todo el mundo. Al mismo tiempo, el aprendizaje electrónico se usa para complementar el aprendizaje cara a cara en entornos tradicionales como las universidades, lo que resulta en un aprendizaje combinado. Si bien no puede reemplazar a la educación tradicional, el aprendizaje electrónico brinda nuevas posibilidades, especialmente cuando las restricciones de tiempo y espacio impiden la asistencia a clase en persona. Recientemente, la educación en línea ha estado vinculada a la reforma de la educación superior, así como también a cambios institucionales y organizacionales.[23]

Tradicionalmente, la educación ha sido gobernada por las instituciones nacionales. La acreditación de instituciones educacionales, el reconocimiento de los títulos y certificaciones, y la garantía de calidad se rigen a nivel nacional. Sin embargo, la educación transfronteriza exige el desarrollo de nuevos regímenes de gobernanza. Muchas iniciativas internacionales tienen el objetivo de suplir deficiencias gubernamentales, especialmente en áreas como la garantía de calidad y el reconocimiento de títulos académicos.

Los asuntos

La OMC y la educación

Un tema controvertido en las negociaciones de la OMC es la interpretación de los Artículos I (3)(b) y 3(c) del Acuerdo General sobre el Comercio de Servicios (AGCS), que especifican las excepciones del régimen de comercio libre para los servicios prestados por el gobierno. De acuerdo con un punto de vista, apoyado principalmente por EE.UU. y el Reino Unido, estas excepciones deberían ser tratadas en sentido estricto, permitiendo *de facto* el libre comercio en la educación superior. Esta perspectiva está en su mayor parte regida por los intereses del sector educacional angloparlante para obtener cobertura de mercado global en la educación, y ha recibido una considerable oposición por parte de muchos países.[24]

Uno de los aspectos clave del debate se centra en si la educación debería ser considerada un producto o un bien social. Si se considera que la educación es un producto, las reglas de libre comercio de la OMC serían implementadas en este campo también. Por el contrario, si se la considera un bien público, se preservaría el modelo actual de la educación, en el que las universidades públicas reciben un estatus especial como instituciones de gran importancia para la cultura nacional. La educación en línea también podría verse afectada por

la liberalización del comercio. Algunos comentaristas han advertido acerca de un posible «deslizamiento del comercio» en la política educativa.[25]

Garantía de calidad y estandarización

La disponibilidad de sistemas de concesión de aprendizaje electrónico y de fácil entrada a este mercado ha abierto la cuestión de la garantía de calidad. Un especial enfoque en los aspectos técnicos de tal servicio en línea puede pasar por alto la importancia de la calidad de los materiales y la didáctica. Una serie de posibles dificultades podría poner el peligro la calidad de la educación. Una de estas dificultades es la fácil entrada a este mercado de nuevas instituciones educativas (generalmente motivadas por propósitos comerciales) que en la mayoría de los casos cuentan con escasas capacidades académicas y didácticas que son necesarias. Otro problema de la garantía de calidad es que la simple transferencia del material ya existente en formato papel al formato digital no aprovecha el potencial didáctico específico de este nuevo medio. Este aspecto ha impulsado a organizaciones educativas a comenzar a desarrollar estándares y directrices para la evaluación del diseño y el contenido de los cursos proporcionados en línea.[26]

El reconocimiento de los títulos académicos y la transferencia de créditos

El reconocimiento de títulos se ha convertido en un asunto de especial relevancia en el contexto del aprendizaje en línea. En dicho contexto, el principal desafío está en el reconocimiento de títulos a nivel regional y global.

La UE ha desarrollado un marco regulatorio a través del Sistema europeo de transferencia y acumulación de créditos (ECTS, por sus siglas en inglés).[27] La región Asia-Pacífico ha implementado su propio modelo regional para el intercambio de alumnos y un sistema de créditos acorde – el programa de Movilidad universitaria en Asia y el Pacífico (UMAP, por sus siglas en inglés).[28]

En la evolución de la implementación del aprendizaje en línea, existe una tendencia hacia el reconocimiento y la transferencia de créditos de conformidad con estrategias clásicas para las universidades tradicionales.

La innovación de los Cursos Masivos Abiertos en Línea (MOOC, por sus siglas en inglés) también está evolucionando, debido a que el ciclo de aceptación inicial generalizada y promoción llegó a su fin, y se están desarrollando más recursos para brindar las mismas o mejores interacciones personales que las que se garantizan en los sistemas educacionales de aprendizaje tradicional o combinado.

La estandarización del aprendizaje en línea

La etapa más temprana en el desarrollo del aprendizaje en línea estuvo caracterizada por el rápido crecimiento y la gran diversidad de plataformas, contenido, y didáctica. Sin embargo, existe la necesidad de crear estándares comunes para facilitar el reconocimiento de los créditos u otros títulos y certificaciones, y de asegurar una calidad mínima. La mayor parte de la estandarización se lleva a cabo por instituciones privadas y profesionales.

TIC, educación, y desarrollo

Los Objetivos de Desarrollo Sostenible (ODS) incluyen un objetivo ambicioso que exige una educación de calidad inclusiva y equitativa, y exige asegurar oportunidades de

aprendizaje permanentes para todos (objetivo 4). La consecución de este objetivo puede estar vinculada a varias líneas de acción de la CMSI, como se muestra en la matriz CMSI-ODS.[29] Esto, a su vez, hace hincapié en la importancia de las TIC para la educación.

www.igbook.info/onlineeducation

Diversidad cultural

La diversidad cultural es un concepto amplio, y puede incluir la diversidad de idiomas, identidades nacionales, tradiciones, y religiones. Existe una relación de doble vínculo entre la Internet y la diversidad cultural, en sus diversas formas. Por un lado, la Internet puede contribuir a la promoción de la diversidad cultural a nivel global, a través de su capacidad para facilitar los intercambios entre personas con diferentes orígenes culturales, y el acceso a vastos recursos de información y conocimiento. La Internet también ofrece a los individuos nuevas posibilidades de expresión en maneras que reflejan sus identidades nacionales y culturales. Por el otro, y como se destacó durante la CMSI, la diversidad cultural es esencial para el desarrollo de una sociedad de la información inclusiva, basada en el diálogo y el respeto entre las culturas.

En el entorno en línea, la preservación, la mejora, y el fomento de la diversidad cultural pueden lograrse, entre otras cosas, incentivando el desarrollo de contenido local. Debido a que el contenido local tiene el potencial de reflejar las identidades nacionales y las especificidades culturales, contar con más contenido local en línea significa contar con adicionales oportunidades para hacer de la Internet un espacio más diverso e inclusivo, y para promover estas mismas identidades y especificidades a nivel global.

La traducción, adaptación, y distribución en línea del contenido local existente, y la preservación de información variada que refleja el conocimiento y las tradiciones indígenas mediante el uso de medios digitales representan otras maneras de promover la diversidad cultural. Los archivos digitales también pueden contribuir a fortalecer a las comunidades locales, y a documentar y preservar la herencia cultural. Esto es particularmente importante para las comunidades aisladas o nómades, cuyas necesidades tecnológicas podrían requerir enfoques que estén completamente localizados. La producción y distribución de s*oftware* en los idiomas locales también tiene el potencial de incrementar las tasas de adopción de la Internet.

www.igbook.info/culturaldiversity

Multilingüismo

Desde sus comienzos, la Internet ha sido un medio predominantemente de la lengua inglesa. Según algunos datos estadísticos, un poco más del 50% del contenido web está en inglés,[30] mientras que el 75% de nuestra población mundial no es angloparlante.[31] Al mismo tiempo, el chino – el idioma más hablado del mundo – representa solo aproximadamente un 2% de todo el contenido. Un informe publicado por la Comisión sobre la Banda Ancha de la ONU en 2015 revela que solo aproximadamente un 5% de los 7100

idiomas que se estima existen en el mundo están representados actualmente en la Internet. También detalla que la escritura latina continúa siendo un desafío para muchos usuarios de la Internet, en particular para la lectura de los nombres de dominio.[32]

Esta situación ha impulsado a varios países a adoptar acciones concertadas para promover el multilingüismo y proteger la diversidad cultural. El fomento del multilingüismo (Figura 23) no solo es un asunto cultural; está directamente relacionado con la necesidad de mayores desarrollos en la Internet. Si el destino de la Internet es que sea usada por más partes de la sociedad, el contenido, entonces, deberá estar disponible en más idiomas.

Aunque el inglés tiene todavía mayor representación en la web, esto está comenzando a cambiar poco a poco. Ya que cada vez más gente se conecta, algunos idiomas se están volviendo más prominentes. Por ejemplo, entre 2011 y 2015, el contenido en ruso demostró un crecimiento del 41,5%, el español creció un 15,5%, y el portugués, un 56%.[33] El rápido incremento en los usuarios de la India y China podría, de la misma manera, llevar a un crecimiento en la base de idiomas en línea del hindú y el chino.

Los asuntos

Alfabetos no latinos

El fomento del multilingüismo requiere estándares técnicos que faciliten el uso de varios alfabetos, escrituras, y caracteres. Una de las primeras iniciativas relacionadas con el uso multilingüe de las computadoras fue tomada por Unicode Consortium – una institución sin fines de lucro que desarrolla estándares para facilitar el uso de conjuntos de caracteres

Figura 23. Multilingüismo

para diferentes idiomas. ICANN y la IETF dieron un importante paso con la introducción de dominios de nivel superior IDN (tanto para los ccTLD como para los gTLD).

Los IDN facilitan el uso de nombres de dominio escritos en alfabetos no latinos (como el chino, el arábico, y el cirílico), así como también con caracteres basados en alfabetos latinos con diacríticos o ligaduras (presentes en idiomas como el francés, el alemán, el húngaro, el rumano, etc.).[34]

Consulte la Sección 2 para obtener más información acerca de los IDN.

Los IDN ayudan a que la Internet sea más inclusiva, ya que la posibilidad de acceder y registrar nombres de dominio en más idiomas y escrituras empodera a más personas a usar la Internet. Los nombres de dominio no solo se basan en direcciones y nombres, sino también en contenido. Por lo tanto, son relevantes para las comunidades locales, y tienen el potencial de fomentar el uso y el desarrollo de contenido local, en idiomas y escrituras locales.

Traducción automática

Se han llevado a cabo varios intentos para mejorar la traducción automática. Dada su política que establece que se deben traducir todas las actividades oficiales a los idiomas de todos los estados miembros, la UE ha apoyado las actividades de desarrollo en el campo de la traducción automática. Aunque ha habido muchos avances (que implican, por ejemplo, el uso de sistemas de IA), todavía existen limitaciones.

Gracias a las crecientes oportunidades de mercado en países no angloparlantes, las compañías de Internet han también comenzado a proporcionar herramientas de traducción automática a sus plataformas. Por ejemplo, Facebook e Instagram brindan traducciones automáticas del contenido generado por el usuario.

Marcos de gobernanza adecuados

El fomento del multilingüismo exige marcos de gobernanza adecuados. El primer elemento de los regímenes de gobernanza ha sido proporcionado por organizaciones como la UNESCO, que ha dado comienzo a muchas iniciativas que se enfocan en el multilingüismo, inclusive la adopción de documentos importantes, como la Declaración Universal sobre la Diversidad Cultural de 2001.[35] Otro impulsor clave del multilingüismo es la UE, ya que lo representa como uno de sus principios fundamentales políticos y laborales.[36]

La evolución y el amplio uso de herramientas web 2.0, que permite a los usuarios convertirse en colaboradores y desarrolladores de contenido, ofrece una oportunidad para una mejor disponibilidad de contenido local en una gran variedad de idiomas. No obstante, sin un marco más amplio para la promoción del multilingüismo, esta oportunidad podría resultar en una brecha incluso más grande, ya que los usuarios sentirían la presión de usar un idioma común (por lo general el inglés) para alcanzar una mayor audiencia.

Acceso significativo

La necesidad de contar con una diversidad lingüística y cultural en la Internet es también un tema importante ligado al acceso y al desarrollo. La disponibilidad de contenido

local, proporcionado en el idioma local, incentiva a las personas a conectarse a Internet. Al mismo tiempo, les permite expresarse en línea en sus propios idiomas y generar contenido. Consecuentemente, el contenido local puede llevar a que la Internet sea un medio más inclusivo y que ayude a reducir la brecha digital existente.

www.igbook.info/multilingualism

Bienes públicos globales

Se han llevado a cabo varios intentos para definir y proteger a la Internet como servicio global y público. El concepto de bien público global es el que se usa con mayor frecuencia además de *res communis omnium,* común global, y la herencia común de la humanidad. Estos conceptos se usan indistintamente y, a su vez, se superponen. La Internet como un bien público global se define por dos enfoques: el económico – como un recurso que carece de rivalidad y de exclusión en su uso; y el de seguridad – como una infraestructura global que traspasa la soberanía nacional.

Enfoque económico

El enfoque económico de la Internet como un bien público global se basa en dos características: la falta de rivalidad (su uso por parte de un individuo no limita el uso de otro individuo) y la falta de exclusión (resulta difícil, si no completamente imposible, excluir a un individuo del goce de este bien). Con este criterio, el Banco Mundial[37] sostiene que la Internet es un bien público imperfecto, ya que solamente posee una de las características de los bienes públicos: la de la no rivalidad, en la que su uso por un individuo no reduce la disponibilidad de este para otros individuos. La Internet no cumple con la otra característica: la de la no exclusión, en donde el uso de la Internet se ve típicamente limitado por el pago de una tarifa, de una manera u otra.

Sin embargo, la Internet no es una entidad unificada sino que tiene varios aspectos. En consecuencia, el estatus que posee como un bien público global podría aplicarse al acceso general de la Internet, el uso de conocimiento y datos en la Internet, el uso de los estándares de la Internet, el acceso a educación en línea, etc.

Una de las características clave de la Internet es que mediante la interacción de sus usuarios en todas partes del mundo, se crean nuevos conocimientos e informaciones. Se ha producido una gran cantidad de conocimiento gracias a intercambios en las listas de correos, redes sociales, y blogs. A excepción de Creative Commons,[38] no existe un mecanismo que facilite el uso legal de tales conocimientos. Abandonado en una incertidumbre jurídica, el conocimiento se pone a disposición para su modificación y comercialización. Esta reserva de conocimiento, que es una base importante para la creatividad, está en riesgo de agotarse. Mientras más se comercializa el contenido de Internet, menos espontáneos se vuelven los intercambios, lo que podría llevar a una interacción creativa reducida.

El concepto del bien público global, combinado con iniciativas como la de Creative Commons, podría brindar soluciones para proteger el actual entorno creativo de la Internet y, a la vez, preservar el conocimiento generado a través de esta para futuras generaciones.

Enfoque de seguridad

El enfoque de la seguridad tiene como objetivo proteger la infraestructura global de la Internet, al considerarla un bien público global. De acuerdo con esta postura, la Internet como bien público global debería estar – en particular – protegida contra la intervención de gobiernos nacionales. Los que apoyan esta teoría a menudo proponen una analogía entre el mar abierto y la Internet.

Consulte la Sección 1 para obtener más información acerca de las analogías.

Típicamente, el enfoque de la seguridad cubre el DNS, el enrutamiento, y los protocolos de la Internet como bienes públicos globales.[39] Los estándares de Internet (principalmente el TCP/IP) son abiertos y públicos. Se dice que el régimen de gobernanza de Internet debería garantizar la protección de los principales estándares de la Internet como bienes públicos globales.

El equilibrio entre los intereses privados y públicos

Uno de los desafíos subyacentes del futuro desarrollo de Internet es lograr un equilibrio entre los intereses privados y los públicos. La pregunta es cómo brindarle al sector privado un entorno comercial apropiado mientras que se asegura el desarrollo de Internet como un bien público global. En muchos casos, no se trata de un juego de suma cero sino de una situación beneficiosa para todos. Muchas compañías de Internet han intentado desarrollar modelos de negocio que provean ingresos y que permitan el desarrollo creativo de la Internet.

Las compañías privadas son predominantes en lo que respecta a la gestión de la infraestructura de Internet. Uno de los desafíos resultantes es la armonización de la propiedad privada de la infraestructura de Internet con el estatus de la Internet como bien público global. Algunas regulaciones nacionales brindan la posibilidad de que la propiedad privada esté restringida por ciertos requisitos públicos, como la igualdad de derechos para todos los potenciales usuarios y la no interferencia del contenido transportado.

www.igbook.info/publicgoods

NOTAS FINALES

[1] Freedom House publica informes anuales *Freedom on the Net*, que investigan, además de otros temas, si los gobiernos de todo el mundo implementan políticas de censura; y si lo hacen, de qué manera. Freedom House (no date) About Freedom on the Net 2015. Disponible en https://freedomhouse.org/report-types/freedom-net [accedido el 2 de Noviembre de 2016].

[2] La iniciativa OpenNet recopila, analiza, y publica datos sobre el filtrado en Internet y sobre prácticas de vigilancia llevadas a cabo en países alrededor del mundo. Provee perfiles de los países, revisiones regionales, y mapas interactivos. Accesible mediante su sitio web https://opennet.net/ [accedido el 2 de septiembre de 2016].

[3] Operación Clambake (sin fecha). Church of Scientology Censors Net Access for Members. Disponible en http://www.xenu.net/archive/events/censorship/ [accedido el 29 de octubre de 2016].

[4] Taylor J (2013) Australian Christian Lobby urges Coalition rethink on Internet filtering. *ZDNet*, 6 de septiembre. Disponible en http://www.zdnet.com/article/australian-christian-lobby-urges-coalition-rethink-on-Internet-filtering/ [accedido el 29 de octubre de 2016].

[5] Aunque Vint Cerf participó en el panel, se opuso al informe final, diciendo que no se enfocaba en las fallas o las mayores implicancias de la instalación de portales en línea. Fuente: Guernsey L (2001) Welcome to the world wide web, passport, please? *New York Times,* 15 de marzo de 2001. Disponible en http://www.nytimes.com/2001/03/15/technology/welcome-to-the-web-passport-please.html?pagewanted=all&src=pm [accedido el 29 de octubre de 2016].

[6] Waddell K (2016) Why Google Quit China – and Why It's Heading Back. *The Atlantic*, 19 de enero. Disponible en http://www.theatlantic.com/technology/archive/2016/01/why-google-quit-china-and-why-its-heading-back/424482/ [accedido el 5 de septiembre de 2016].

[7] Un buen punto de partida para este debate es la publicación de Mary Murphy en el canal de blogs de Gobernanza de Internet de DiploFoundation y los comentarios que surgieron: *Google... stop thinking for me!* Disponible en https://www.diplomacy.edu/blog/googlestop-thinking-me [accedido el 29 de octubre de 2016].

[8] Connolly K (2016) Angela Merkel: Los motores de búsqueda de Internet están distorsionando nuestra percepción de la realidad. *The Guardian*, 27 de octubre. Disponible en https://www.theguardian.com/world/2016/oct/27/angela-merkel-Internet-search-engines-are-distorting-our-perception [accedido el 30 de octubre de 2016].

[9] Crete-Nishihata M and York J (2011) Censura de Internet en Egipto: ejemplo extremo de un bloqueo justo a tiempo. Iniciativa OpenNet. Disponible en http://opennet.net/blog/2011/01/egypt%E2%80%99s-Internet-blackout-extreme-example-just-time-blocking [accedido el 29 de octubre de 2016].

[10] Facebook (2015) Declaración de Derechos y Responsabilidades. Facebook, 30 de enero. Disponible en https://www.facebook.com/terms [accedido el 14 de julio de 2016].

[11] Greenberg A (2016) Inside Google's Internet justice league and its AI-powered war on trolls. *Wired*, 9 de septiembre. Disponible en https://www.wired.com/2016/09/inside-googles-Internet-justice-league-ai-powered-war-trolls/ [accedido el 30 de octubre de 2016].

[12] Chazan D (2016) Facebook, YouTube y Twitter demandados por no eliminar contenido homófobo. *The Telegraph*, 15 de mayo. Disponible en http://www.telegraph.co.uk/news/2016/05/15/facebook-youtube-and-twitter-sued-for-failure-to-remove-homophob/ [accedido el 14 de julio de 2016].

[13] Williams D (2016) Relatives of Palestinian attack victims sue Facebook for $1 billion in U.S. *Reuters*, 11 de julio. Disponible en http://www.reuters.com/article/us-israel-palestinians-facebook-idUSKCN0ZR1G0 [accedido el 14 de julio de 2016].

[14] *BBC* (2016) Twitter, Facebook y Google colaboraron en los ataques en París. 16 de junio de 2016. Disponible en http://www.bbc.com/news/technology-36548798 [accedido el 14 de julio de 2016].

[15] G7 (2016) Plan de Acción del G7 para contrarrestar el terrorismo y el extremismo violento. Disponible en http://www.mofa.go.jp/files/000160278.pdf [accedido el 18 de agosto de 2016].

[16] Centro de Noticias de la ONU (2016) El Consejo de Seguridad le solicita al panel de la ONU proponer un marco global en la lucha contra la propaganda terrorista. 11 de mayo. Disponible en http://www.un.org/apps/news/story.asp?NewsID=53909#.V7VzGWW5oQF [accedido el 18 de agosto de 2016].

[17] UNODC (2012) *El uso de la Internet con fines terroristas*. Viena: Oficina de las Naciones Unidas en Viena. Disponible en https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf [accedido el 18 de agosto de 2016].

[18] Consejo de Europa (2003) Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. Disponible en http://conventions.coe.int/Treaty/en/Treaties/html/189.htm [accedido el 29 de octubre de 2016].

[19] Comisión Europea (2015) De una Internet más segura a una mejor Internet para los niños. Disponible en http://ec.europa.eu/digital-agenda/en/safer-Internet-better-Internet-kids [accedido el 29 de octubre de 2016].

[20] Para obtener más detalles sobre las diferentes implicaciones del filtrado de contenido, consulte: Comité Asesor de la Seguridad y Estabilidad de ICANN (2012) SSAC Recomendación sobre los impactos del bloqueo de contenido a través del Sistema de Nombres de Dominio. Disponible en https://www.icann.org/en/system/files/files/sac-056-en.pdf [accedido el 5 de septiembre de 2016], y Barnes A *et al*. (2016) Consideraciones técnicas para el bloqueo y el filtrado de sistemas de Internet (Junta de Arquitectura de Internet RFC 7754). Disponible en https://tools.ietf.org/html/rfc7754 [accedido el 5 de septiembre de 2016].

[21] Yadron D and Wong JC (2016) Silicon Valley appears open to helping US spy agencies after terrorism summit. *The Guardian*, 8 de enero. Disponible en https://www.theguardian.com/technology/2016/jan/08/technology-executives-white-house-isis-terrorism-meeting-silicon-valley-facebook-apple-twitter-microsoft [accedido el 18 de agosto de 2016].

[22] Comisión Europea (2016) La Comisión Europea y las compañías TIC anuncian un Código de Conducta para combatir la propagación de mensajes de odio ilegales en línea. Disponible en http://europa.eu/rapid/press-release_IP-16-1937_en.htm [accedido el 18 de agosto de 2016].

[23] Willcox K *et al*. (2016) Educación en línea: Un catalizador para la reforma de la educación superior. Instituto Tecnológico de Massachusetts. Disponible en https://professional.mit.edu/sites/default/files/MIT%20Online%20Education%20Policy%20Initiative%20April%202016.pdf [accedido el 18 de agosto de 2016].

[24] Para un estudio completo de la interpretación de AGCS relacionado con la educación superior, lea Tilak J (2011) *Comercio en la educación superior: El rol del Acuerdo General sobre el Comercio de Servicios (AGCS)*. París: UNESCO, Instituto Internacional de Planeamiento de la Educación. Disponible en http://unesdoc.unesco.org/images/0021/002149/214997e.pdf [accedido el 29 de octubre de 2016].

[25] Knight J (2015) Trade creep: Implications of GATS for higher education policy. *International Higher Education* 28, pp. 5–7. Disponible en http://ejournals.bc.edu/ojs/index.php/ihe/article/view/6658 [accedido el 29 de octubre de 2016].

[26] Para obtener una lista de muestra de las organizaciones y los trabajos que abordan las recomendaciones y estándares para el aprendizaje electrónico, consulte WBTIC (sin fecha) Overview of E-learning Standards. Disponible en http://wbtic.com/primer_standards.aspx [accedido el 29 de octubre de 2016].

[27] Comisión Europea (sin fecha) ECTS. Disponible en http://ec.europa.eu/education/tools/ects_en.htm [accedido el 29 de octubre de 2016].

[28] UMAP (sin fecha) UMAP. Disponible en http://umap.org/about/ [accedido el 29 de octubre de 2016].

[29] Foro CMSI (2015) Matriz CMSI-ODS: Uniendo las líneas de acción de la CMSI con los Objetivos de Desarrollo Sustentable. Ginebra: Unión Internacional de las Telecomunicaciones. Disponible

en https://www.itu.int/net4/wsis/sdg/Content/wsis-sdg_matrix_document.pdf [accedido el 27 de octubre de 2016].

30 W3Techs (2016) Usage of content languages for websites. Disponible en https://w3techs.com/technologies/overview/content_language/all [accedido el 29 de octubre de 2016].

31 Centro de Políticas de la Academia Británica (2011) Language Matters More and More. Disponible en http://www.ucml.ac.uk/sites/default/files/pages/160/Language%20Matters%20more%20and%20more.pdf [accedido el 29 de febrero de 2016].

32 La Comisión sobre Banda Ancha para el Desarrollo Digital (2015) El estado de la banda ancha de 2015: Broadband as a Foundation for Sustainable Development. Disponible en http://www.broadbandcommission.org/Documents/reports/bb-annualreport2015.pdf [accedido el 18 de agosto de 2016].

33 Wood J (2015) Top languages of the Internet, today and tomorrow. *Unbabel*, 10 de junio. Disponible en https://blog.unbabel.com/2015/06/10/top-languages-of-the-Internet/ [accedido el 15 de julio de 2016].

34 Para obtener un resumen del programa IDN, así como también actualizaciones relacionadas con su implementación, consulte ICANN (sin fecha) Nombres de Dominio Internacionalizados. Disponible en https://www.icann.org/resources/pages/idn-2012-02-25-en [accedido el 29 de octubre de 2016].

35 UNESCO (2001) Declaración Universal sobre la Diversidad Cultural. Disponible en http://portal.unesco.org/en/ev.php-URL_ID=13179&URL_DO=DO_TOPIC&URL_SECTION=201.html [accedido el 29 de octubre de 2016].

36 Comisión Europea (sin fecha) Multilingüismo. Disponible en http://ec.europa.eu/languages/index_en.htm [accedido el 29 de octubre de 2016].

37 Banco Mundial (2016) Informe sobre el Desarrollo Mundial 2016: El dividendo Digital. Disponible en http://www.worldbank.org/en/publication/wdr2016 [accedido el 29 de febrero de 2016].

38 Creative Commons es una organización sin fines de lucro que desarrolla, apoya, y administra la infraestructura legal y técnica que maximiza la creatividad, el intercambio, y la innovación digitales. Disponible en http://creativecommons.org/ [accedido el 29 de octubre de 2016].

39 Broeders D (2015) *The public core of the Internet*. Ámsterdam: Amsterdam University Press. Disponible en http://www.wrr.nl/fileadmin/en/publicaties/PDF-Rapporten/The_public_core_of_the_Internet_Web.pdf [accedido el 31 de octubre de 2016].

Sección 8

LA CANASTA DE DERECHOS HUMANOS

La canasta de derechos humanos

El conjunto básico de derechos humanos relacionados con Internet incluye la privacidad; la libertad de expresión; el derecho a buscar, recibir, e impartir información; varios derechos que protegen la diversidad cultural, lingüística y minoritaria; y el derecho a la educación. Otros derechos humanos entran en escena en el ámbito de las políticas digitales, como los derechos de los niños, y los derechos reconocidos para los periodistas y la prensa.

Si bien los derechos humanos siempre se abordan de manera explícita (por ejemplo, la libertad de expresión y la privacidad en línea), también están involucrados en temas transversales que aparecen al lidiar con la neutralidad de la red (el derecho al acceso, a la libertad de expresión, al anonimato), la ciberseguridad (la observancia de los derechos humanos al llevar a cabo actividades relativas a la ciberseguridad y la protección), el control de contenido, etc.

Derechos humanos fuera de línea vs en línea

Las resoluciones de la Asamblea General y el Consejo de Derechos Humanos (CDH) de la ONU, al igual que otros documentos similares adoptados dentro de organizaciones regionales como el CdE y la UE, han establecido firmemente el principio de que los derechos humanos que las personas ejercen *fuera de línea*, también deben ser protegidos *en línea*. La Asociación para el Progreso de las Comunicaciones (APC) destaca, en la Carta sobre derechos en Internet, que los derechos humanos relacionados con Internet están incorporados en el sistema de derechos humanos de la ONU basado en la Declaración Universal de los Derechos Humanos (DUDH) y otros instrumentos conexos.[1]

Mientras que la cuestión de los derechos fuera de línea vs los derechos en línea ha sido resuelta en principio, la implementación de la regulación fuera de línea en el espacio en línea plantea nuevos desafíos. Aquellos que sugieren que los derechos en línea exigen un enfoque específico afirman que la mera cantidad de la comunicación facilitada por la Internet (es decir, la intensidad de la comunicación, la cantidad de mensajes) representa una diferencia cualitativa. Por ejemplo, el problema del discurso del odio no es una cuestión de si la regulación en su contra se puede legislar o no, sino que de la facilidad de compartir y difundir el discurso del odio a través de Internet lo convierte en otro tipo de problema legal. A medida que más individuos están expuestos a los discursos de odio a través de numerosas plataformas en línea, se hace cada vez más difícil hacer cumplir las normas existentes contra el discurso de odio. Por lo tanto, por más de que las reglas existentes sean adecuadas, la Internet impone desafíos relacionados con la aplicación de estas.

Tecnología y derechos humanos

Los estándares y protocolos técnicos afectan el ejercicio de los derechos humanos. Los proveedores de infraestructuras, los fabricantes de dispositivos, y los órganos de estandarización tienen un rol por desempeñar en la definición de las protecciones recogidas en la capa

técnica de Internet. Los mecanismos y protocolos de cifrado como «Do Not Track» pueden hacer que el valor por defecto sean la protección de la privacidad y la libertad de expresión.

A nivel del DNS, surgieron controversias, por ejemplo, con el lanzamiento del dominio de nivel superior .sucks (apesta, en español), aprobado por ICANN en febrero de 2015. Algunos han criticado este desarrollo por su potencial de extorsión (el pago de premiums para adquirir un nombre de dominio de segundo nivel de tipo [marca].sucks), mientras que otros lo toman como un espacio para el ejercicio de la libertad de expresión.[2] Esta y otras cuestiones por el estilo resultaron en intensos debates dentro de la comunidad de ICANN que se centraban en que si ICANN, como una organización técnica *per se,* debería tener obligaciones relacionadas con los derechos humanos. Los estatutos de ICANN de 2016 incorporan a los derechos humanos entre los valores centrales que deben guiar las decisiones y acciones de ICANN. ICANN debe respetar los «derechos humanos reconocidos internacionalmente como lo exige la ley aplicable». De todas maneras, queda puesto de relieve que este valor central no crea ninguna obligación para ICANN fuera de su misión (que es « asegurar la operación estable y segura de los sistemas de identificadores únicos de Internet») u obligaciones que van más allá de la ley aplicable.[3]

«Nuevos» derechos humanos gracias a Internet

El derecho al acceso

Estonia fue el primer país que garantizó jurídicamente el derecho al acceso a Internet mediante una legislación de servicio universal, en el 2000. En julio de 2010, Finlandia dio a sus ciudadanos un derecho legal a una conexión de banda ancha de 1 Mbps (la velocidad se duplicó a 2 Mbps a partir de noviembre de 2015). Otros países han dado pasos similares para garantizar a sus ciudadanos el derecho al acceso a Internet.[4] Las opiniones todavía difieren en cuanto a un reconocimiento mundial sólido del acceso a Internet como un derecho humano. Algunos argumentan que el acceso a Internet no puede tener el mismo peso que el acceso al agua potable, la comida, y otras necesidades básicas. Otros afirman que este es un falso dilema, ya que el acceso a Internet es a menudo esencial para asegurar la satisfacción de otros derechos humanos básicos.

La neutralidad de la red y la tasación cero han hecho que el derecho al acceso se ubique en el centro de la atención pública en todo el mundo. ¿A qué tipo de acceso a Internet nos referimos cuando hablamos del derecho al acceso? ¿Deberíamos considerar que el acceso a un número limitado de sitios web y plataformas, como el que brindan las aplicaciones sin cargo, es acceso a Internet? La respuesta del gobierno de la India a esta pregunta fue negativa, al prohibir los servicios a tasa cero. Otros países están debatiendo esta temática. Queda por ver cuál de los siguientes ángulos domina la discusión sobre la tasación cero: los derechos humanos (derecho al acceso), la economía (modelo de negocio emergente), o el desarrollo (apoyo a comunidades desfavorecidas).

El derecho al olvido

El derecho al olvido, o más precisamente el derecho a la desindexación, fue introducido por el caso icónico del TJUE C-131/12 Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos (AEPD) y Mario Costeja González. El caso tuvo que ver con un anuncio de subasta publicado por el periódico español *La Vanguardia* para la propiedad del

señor Costeja debido a deudas impagas en 1998. Aunque Costeja había saldado sus deudas muchos años antes, una vez que el periódico digitalizó sus archivos, cualquier búsqueda de Google que contuviera su nombre apuntaba al anuncio de subasta entre los primeros resultados. La corte española de primera instancia decidió que los archivos del periódico debían permanecer inalterados en relación con la exposición de esta información: se consideró como una cuestión de libertad de prensa. Sin embargo, la Agencia Española de Protección de Datos exigió que Google removiera el enlace que llevaba a esta información. Google impugnó este fallo mediante una audiencia nacional, que dirigió el caso al TJUE.

El 13 de mayo de 2014, el fallo del TJUE contra Google procedió de la siguiente manera: En primer lugar, aseveró su competencia jurisdiccional estableciendo que las actividades del motor de búsqueda de la subsidiaria española de Google Inc. – con sede principal en EE. UU. y propietaria del algoritmo de búsqueda – eran «económicamente rentables» y entraban dentro del alcance territorial de aplicación de la Directiva de Protección de Datos 95/46 de la UE. En segundo lugar, determinó que Google era un gestor de datos (una entidad de procesamiento de datos), ya que su actividad consistía en «localizar la información publicada o incluida en la red por terceros, indexarla de forma automática, almacenarla temporalmente, y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia». En tercer lugar, exigió que Google cumpliera con la Directiva de Protección de Datos como el gestor sobre el territorio de un estado miembro de la UE, para «eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en sí misma en dichas páginas sea lícita».[5] El Tribunal también reconoció que cuando entra en juego el interés público, el gestor de datos necesita evaluar la continuación de la disponibilidad de un enlace en particular.

Mediante este proceso, el TJUE introdujo un nuevo enfoque que depende del procesamiento de datos según la ubicación del usuario, independientemente de la ubicación del servidor o de la sede central de la compañía.[6] Este fue un punto de fricción en los meses que siguieron a la sentencia del TJUE, que llegó a atraer más atención con una orden del Tribunal parisino *Tribunal de Grande Instance* a favor de la aplicabilidad global, lo que forzó a Google a trasladarse desde la desindexación de resultados desde sus subdominios entre la UE (google.it, google.fr) a la remoción de enlaces de google.com cuando el acceso ocurra desde Europa.[7]

Además la UE dio un paso más adelante, consagrando el derecho al olvido en la legislación, con la adopción de un nuevo Reglamento sobre la protección de datos (que reemplazó a la Directiva de 1996).[8] Este Reglamento, que será aplicable a partir de mayo de 2018, contiene disposiciones específicas sobre el «derecho de supresión (derecho al olvido)», que indica que los individuos tienen el derecho de obtener la supresión de sus datos personales por varios motivos, y que el gestor tiene la obligación de eliminar dichos datos sin demora indebida. Además, si el gestor hizo públicos los datos personales, se requiere también que dé «los pasos razonables» para informar a los gestores que procesan los datos respectivos sobre el hecho de que el titular de los datos ha solicitado la supresión de todos los enlaces, copias, y replicaciones de esos datos personales.

La regulación del derecho al olvido le ha dado su origen a dos opiniones contrarias: algunos la consideran una mejora del derecho a la privacidad y protección de datos, ya que define un proceso por el cual los usuarios pueden solicitar la remoción de los datos recopilados y almacenados por las compañías de Internet. Otros la ven como una posible amenaza para

la libertad de expresión, en el caso de que las disposiciones legales se implementen de una manera en la que permitan que el contenido sea eliminado incluso si no existe la violación de los derechos de otra persona.[9] Queda por ver cómo se implementarán las disposiciones legales y cuál de estas dos opiniones prevalecerá.

www.igbook.info/hr

Internet y los derechos humanos existentes

La libertad de expresión y el derecho a buscar, recibir, e impartir información

La libertad de expresión en línea ha sido uno de los puntos principales en la agenda diplomática durante los últimos años; se encuentra, por ejemplo, en la agenda del CDH de la ONU, así como también en los órganos intergubernamentales regionales como el CdE. La libertad de expresión en Internet se ha debatido en numerosas conferencias y procesos internacionales, inclusive en las reuniones del IGF. Uno de los enfoques más completos es el de la Freedom Online Coalition (un grupo de 30 gobiernos, en noviembre de 2016), que organiza reuniones anuales y realiza actividades de investigación y sensibilización sobre la libertad de expresión en Internet.

La discusión sobre este tema representa un área de políticas controvertida. La libertad de expresión es uno de los derechos humanos fundamentales, que aparece usualmente en el contexto de los debates sobre control de contenido, censura, y vigilancia por parte del gobierno. Adicionalmente, la cuestión de la libertad de expresión se ve complejizada por algunos enfoques actuales hacia la proliferación del discurso del odio y opiniones extremas en Internet, con argumentos que están tanto a favor como en contra de las medidas destinadas a la limitación del libre discurso en dichos casos.[10] No obstante, parece haber una tendencia hacia la limitación del libre discurso a favor de la responsabilidad social.[11]

La libertad de expresión en línea también abarca otros temas relacionados con la gobernanza de Internet, como el cifrado, el anonimato, la neutralidad de la red, y los IPR. Algunos de estos aspectos han sido analizados en informes emitidos por el Relator Especial de la ONU sobre la promoción y la protección del derecho a la libertad de opinión y expresión, quien hizo énfasis en las numerosas ocasiones en las que el derecho a la libertad de expresión merece una fuerte protección. La libertad de expresión también aparece dentro de debates más amplios sobre derechos humanos y el acceso a Internet.

La protegen instrumentos mundiales, como DUDH (Artículo 19) y el Pacto Internacional de Derechos Civiles y Políticos de la ONU (Artículo 19), e instrumentos regionales como la Convención Europea de Derechos Humanos (Artículo 10) y la Convención Americana de Derechos Humanos (Artículo 13).

En la DUDH, la libertad de expresión se ve contrarrestada por el derecho del estado a limitar la libertad de expresión por razones de moral, orden público, y bienestar general (Artículo 29). Entonces, tanto el debate como la implementación del Artículo 19 deben ser tomados en cuenta dentro del contexto del establecimiento de un equilibrio adecuado

entre dos necesidades.[12] Esta situación ambigua abre muchas posibilidades para las diferentes interpretaciones de normas y, finalmente, de las diferentes implementaciones. La controversia que rodea el equilibrio adecuado entre los Artículos 19 y 29 en el mundo real se ve reflejada en los debates acerca de la consecución de ese balance en Internet.

El principal mecanismo de gobernanza para abordar la libertad de expresión en línea es la Resolución sobre la Protección de la Libertad de Expresión en Internet del CDH de la ONU (2012).

La libertad de expresión es la protagonista de la atención de algunas ONG de derechos humanos como Human Rights Watch, Amnistía Internacional, y Freedom House. Esta última, por ejemplo, evalúa el nivel de libertad en Internet que experimentan los usuarios promedio en países de muestra alrededor del mundo. Su informe Libertad en la Red 2016 señaló que la libertad en Internet en todo el mundo ha disminuido por sexto año consecutivo y más de la mitad de los 65 países evaluados se encontraban en una trayectoria negativa, impulsada por acciones como la censura y restricciones al uso de ciertos servicios de Internet, detenciones de usuarios de redes sociales, amplia vigilancia, y cierre de todo acceso a Internet en casos específicos.[13]

www.igbook.info/foe

Privacidad y protección de datos[14]

La privacidad y la protección de datos son importantes para varias canastas de la gobernanza de Internet: la de derechos humanos, infraestructura (el desarrollo de estándares para la gestión de datos), seguridad (acceso a los datos para la protección de la seguridad nacional y la lucha contra el crimen), y economía (el procesamiento de los datos como la base de un modelo de negocio).

La privacidad y la protección de datos son dos temas de la gobernanza de Internet interrelacionados. La privacidad usualmente se define como el derecho de los ciudadanos a controlar su propia información personal y decidir entre divulgarla o no. La protección de datos es el mecanismo legal que asegura la privacidad. La privacidad es un derecho humano fundamental. Es reconocida en la DUDH, el Pacto Internacional de Derechos Civiles y Políticos, y en muchos otros acuerdos de derechos humanos internacionales y regionales.

Las culturas nacionales y las diferentes formas de vida influyen en la práctica de la privacidad. La privacidad es especialmente importante en las sociedades occidentales. Por ejemplo, en Alemania, se le confiere una relevancia muy alta a la privacidad. Las prácticas modernas de la privacidad se concentran en la privacidad de la comunicación (que no haya vigilancia de la comunicación) y la privacidad de la información (que no se manipule la información sobre los individuos). Tradicionalmente, las preocupaciones sobre la privacidad estaban relacionadas con la vigilancia estatal. Sin embargo, los problemas de la privacidad se relacionan cada vez más con vulneraciones por parte del sector comercial también.

Los asuntos

Los principales asuntos de privacidad se pueden analizar mediante el uso de un triángulo entre individuos, estados, y negocios, como muestra la Figura 24.

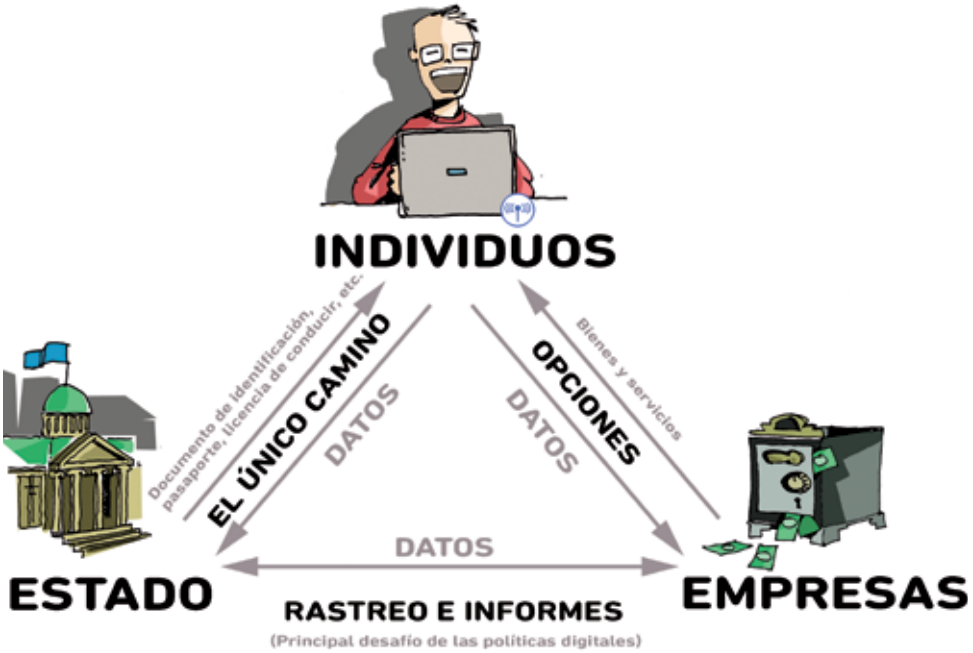

Figura 24. La privacidad en la era digital

Protección de la privacidad: individuos y estados

La información siempre ha sido una herramienta esencial para que los estados ejerzan la autoridad sobre sus territorios y poblaciones. Los gobiernos recopilan grandes cantidades de información personal (registros de nacimiento y casamiento, números de seguro social, inscripción en el patrón electoral, antecedentes penales, información fiscal, registros de vivienda, propiedad de automóviles, etc.). No es posible para un individuo elegir no brindar datos personales al estado, salvo que migre a otro país, en el que se encontraría con la misma solicitud de datos. La tecnología de la información, como la que se usa en la minería de datos,[15] ayuda a la incorporación y correlación de datos provenientes de muchos sistemas especializados (por ejemplo, impuestos, registros de vivienda, propiedad de automóviles) para llevar a cabo análisis sofisticados, en busca de patrones comunes y anormales, e inconsistencias (Figura 25).

Uno de los principales desafíos de las iniciativas del gobierno electrónico es asegurar un equilibrio adecuado entre la modernización de las funciones del gobierno garantizando los derechos a la privacidad de los ciudadanos, incluso la restricción de la recopilación de información a lo que sea estrictamente necesario para desempeñar las funciones legítimas del gobierno y prestar los servicios públicos. Sin embargo, los últimos años presenciaron un mayor apetito del estado por la recopilación de los datos, y la asociación de más datos personales para la identificación obligatoria (como los datos biométricos).

Tras los sucesos del 11 de septiembre de 2001 en EE. UU., la Ley Patriota de EE. UU.[16] y leyes comparables en otros países extendieron la autoridad del gobierno para recopilar información, además de introducir una disposición para la lícita interceptación de la información. El concepto de la interceptación lícita en la recopilación de pruebas también está incorporado en la Convención sobre Cibercrimen del CdE (Artículos 20 y 21).

Protección de la privacidad: individuos y empresas

Como muestra el triángulo de la privacidad (Figura 24), la segunda – y cada vez más importante – relación se da entre los individuos y el sector comercial. Los individuos revelan información personal al abrir una cuenta bancaria, reservar un vuelo o un hotel, pagar con tarjeta de crédito en línea, o incluso navegar en Internet: cada una de estas actividades puede dejar múltiples rastros de datos.

El éxito y sustentabilidad del comercio electrónico, tanto en la relación empresa-cliente como en la de empresa-empresa, dependen de la construcción de una confianza en las políticas de privacidad y las medidas de seguridad que establecen para proteger la información confidencial de los clientes y prevenir el robo o el uso indebido. Junto con la expansión de las plataformas de redes sociales (por ejemplo, Facebook y Twitter), emergieron preocupaciones sobre el posible uso indebido de los datos personales – no solamente por parte del dueño o administrador de la plataforma de la red social, sino por otros usuarios.[17] Además, las compañías de Internet tienden a cambiar sus políticas de privacidad con regularidad, y no le dan la posibilidad de elegir a sus usuarios, más que la acción del «tómalo o déjalo» (en la que los usuarios aceptan por completo las políticas de privacidad, o deciden dejar de usar el servicio).[18]

En una economía de la información, los datos sobre los consumidores, incluidos sus perfiles de compra y preferencias, se convierten en un importante producto del mercado. Para algunas compañías, como Facebook, Google, y Amazon, la información sobre las preferencias de los consumidores constituye un pilar fundamental para su modelo de negocio. Básicamente, la moneda que los usuarios pagan por los servicios (en línea) considerados «sin costos» son sus datos personales, ya sea en forma de cookie de navegador que indica su comportamiento en línea o información solicitada para completar un formulario web o realizar un pago. A medida que los usuarios revelan más información sobre ellos mismos, más frecuentes y sofisticadas son las violaciones de la privacidad.[19]

Protección de la privacidad: estados y empresas

La tercera parte en el triángulo de la privacidad es la que recibe una menor cantidad de difusión, pero quizás es la más significativa en lo que respecta a la privacidad.

Tanto los estados como las empresas recopilan cantidades importantes de datos sobre los individuos. Los estados ejercen mucha presión sobre las compañías de Internet (por ejemplo, Facebook y Google) para que les confieran acceso a los datos para respaldar sus actividades contra el terrorismo y la delincuencia. A modo de ejemplo, tras los atentados terroristas en París en noviembre de 2015, el gobierno francés dependió en gran medida de los datos provistos por la industria de Internet. Así, los gobiernos están cada vez más preocupados por el cifrado más seguro utilizado por la industria de Internet, que dificulta la vigilancia del tráfico de Internet.

El sector empresarial intenta resistir la presión gubernamental y limitar el acceso de las autoridades estatales a sus datos. Si las autoridades gubernamentales obtienen acceso a los datos de las empresas, esto puede reducir el nivel de confianza entre los usuarios de Internet y afectar el modelo de negocio de las compañías de Internet. La tensión entre las autoridades estatales y el sector empresarial continuará siendo uno de los problemas subyacentes en la política digital global en el futuro próximo.

Figura 25. Minería de datos

Protección de la privacidad: individuos e individuos

El último aspecto de la protección de la privacidad, que no se ve en el triángulo de la privacidad, es el posible riesgo a la privacidad proveniente de los individuos. Actualmente, cualquier persona con los fondos suficientes puede ser dueña de una poderosa herramienta de vigilancia. Incluso un simple teléfono móvil con cámara incorporada puede convertirse en una herramienta de este estilo. Para citar al periódico *The Economist*, la tecnología ha «democratizado la vigilancia».[20] Muchos casos de invasión a la privacidad tuvieron su origen desde el voyerismo hasta el sofisticado uso de cámaras para registrar números de tarjetas en los bancos y para el espionaje económico.

El problema central para la protección en contra de este tipo de violación de la privacidad es que la mayor parte de la legislación se concentra en los riesgos que se originan desde el estado o compañías privadas. Frente a esta nueva realidad, algunos gobiernos han empezado a dar los primeros pasos. El Congreso de EE. UU. promulgó la Ley de Prevención contra el Video Voyerismo,[21] que prohíbe tomar fotografías de gente desvestida sin su consentimiento. Alemania y algunos otros países promulgaron leyes de privacidad similares, con el propósito de prevenir la vigilancia llevada a cabo por individuos.

La regulación internacional de la privacidad y la protección de datos

Uno de los principales instrumentos internacionales sobre la privacidad y la protección de datos es el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal[22] del CdE de 1981. Aunque fue adoptado por una organización regional (CdE), está abierto para la adhesión de estados no europeos. Debido a que el Convenio es neutral en cuanto a la tecnología, ha perdurado en el tiempo.

La Directiva de Protección de Datos de 1995 de la UE[23] también representó un marco legislativo importante para el procesamiento de los datos personales en la UE y tiene un gran impacto sobre el desarrollo de la legislación nacional no solo en Europa sino también en todo el mundo. Tras un proceso de reforma para lidiar con los nuevos desarrollos y asegurar la efectividad de la protección de la privacidad en el ambiente tecnológico actual,

se adoptó un nuevo Reglamento de Protección de Datos en 2016, que entrará en vigor en mayo de 2018, remplazando la Directiva de 1995.[24]

Otro documento internacional clave – pero no vinculante – sobre la privacidad y la protección de datos es el de las Directrices de la OCDE sobre la protección de la privacidad y flujos transfronterizos de datos personales[25] de 1980, actualizadas en 2013. Estas directrices y el trabajo subsiguiente de la OCDE inspiraron muchas regulaciones internacionales, regionales, y nacionales sobre la privacidad y la protección de datos. Al día de hoy, casi todos los países de la OCDE han promulgado leyes de privacidad y empoderado a las autoridades a aplicar dichas leyes.

Aunque los principios de las directrices de la OCDE recibieron una amplia aceptación, existen diferencias en las maneras en que se implementan, especialmente entre Europa y EE. UU. En Europa, existe una legislación integral para la protección de datos, mientras que en EE. UU. la regulación de la privacidad se ha desarrollado para cada sector de la economía, inclusive la privacidad financiera (la ley Graham-Leach-Bliley), la privacidad de los niños (la Ley de la Protección de la Privacidad en Línea de los Niños), y la privacidad médica (bajo la ley de Portabilidad y Contabilidad de Seguro de Salud).

Otra diferencia importante es que, en Europa, la legislación de la privacidad se aplica mediante las autoridades públicas, mientras que en EE. UU., la aplicación recae principalmente sobre el sector privado y la autorregulación. Las empresas establecen sus propias políticas de privacidad, y otras empresas e individuos están a cargo de informarse y actuar de manera acorde. La principal crítica del enfoque de EE. UU. es que los individuos están ubicados en una posición relativamente débil, ya que rara vez son conscientes de la importancia de las opciones proporcionadas por las políticas de privacidad y comúnmente están de acuerdo con ellas sin informarse de manera correcta.

Escudo de Privacidad entre EE. UU. y la UE

Los diferentes enfoques sobre la privacidad de EE. UU. y de la UE plantearon preguntas principalmente relacionadas con el procesamiento de los datos personales por parte de las compañías privadas. ¿Cómo puede asegurar la UE que los datos de sus ciudadanos están protegidos en conformidad con las reglas especificadas en su reglamento de protección de datos? ¿Qué reglas aplican (las de UE o EE. UU.) al tratar con datos transferidos mediante la red de una compañía desde la UE hacia EE. UU.? La UE amenazó con bloquear la transferencia de datos a cualquier país que no pudiera asegurar el mismo nivel de protección de la privacidad como está especificado en su marco legislativo. Esta petición llevó inevitablemente a un choque contra el enfoque estadounidense de autorregulación de la protección de la privacidad.

Esta fundamental diferencia hizo que fuera difícil llegar a cualquier tipo de acuerdo posible. Además, ajustar la legislación estadounidense a la ley de protección de datos de la UE no hubiera sido posible, ya que habría exigido cambiar algunos de los principios fundamentales del sistema legal de EE. UU. La ruptura de este estancamiento se dio en 1998, cuando el embajador de EE. UU., David L. Aaron sugirió la fórmula «Safe Harbour». Esto creó un nuevo marco para el asunto y proporcionó una salida para las negociaciones que estaban en punto muerto.

El Acuerdo Safe Harbour proporcionó un marco jurídico para el intercambio de datos que cruzan el Océano Atlántico. Su finalidad era asegurar que los datos de los ciudadanos de

la UE quedaban protegidos en conformidad con las normas de la UE incluso si los datos se encontraban en servidores ubicados en EE. UU. El acuerdo permitió la aplicación de las normas de la UE en las compañías de EE. UU. dentro de un «puerto seguro» (*safe harbour*). Las compañías estadounidenses que gestionaban los datos de ciudadanos de la UE podían registrarse voluntariamente para cumplir con los requisitos de protección de datos de la UE. Una vez que estuvieron sujetas al acuerdo, tuvieron que cumplir con los mecanismos de aplicación formales acordados entre la UE y EE. UU. En virtud del Safe Harbour, más de 4400 compañías transfirieron datos desde la UE hacia EE. UU. de manera legal durante 15 años.

Sin embargo, en octubre de 2015, el TJUE invalidó el Marco Safe Harbour, ya que consideraba que la Comisión Europea no había evaluado de manera adecuada si EE. UU. mantenía una protección «esencialmente equivalente» de los datos de los ciudadanos de la UE.[26] Esa decisión impulsó negociaciones entre los diplomáticos de la UE y EE. UU. en busca de un nuevo mecanismo. Estas negociaciones le dieron origen al Escudo de Privacidad, aprobado por los estados miembros de la UE en julio de 2016, con cuatro abstenciones: Austria, Bulgaria, Croacia, y Eslovenia. Durante ese mismo mes, la Comisión Europea adoptó formalmente una decisión que confirmó la idoneidad del Escudo de Privacidad entre la UE y EE. UU.[27]

El Escudo impone obligaciones más firmes sobre las compañías estadounidenses para proteger los datos personales de los ciudadanos de la UE, y exige que el gobierno de EE. UU. aplique más estrictamente las disposiciones nuevas y supervise su implementación. Además, el Escudo de Privacidad también aborda un problema que ha presentado un importante motivo de preocupación: el acceso del gobierno de EE. UU. a los datos de los ciudadanos de la UE. El Escudo aportó garantías por escrito por parte de EE. UU. acerca de que tal acceso estaría sujeto a las limitaciones, salvaguardas, y mecanismos de supervisión que correspondan. El gobierno de EE. UU. también se ha comprometido a cooperar con las autoridades de protección de datos en la UE, así como también a crear un mecanismo de defensoría del pueblo para recibir y responder denuncias de las personas en relación con el acceso del gobierno de EE. UU. a sus datos personales.

www.igbook.info/privacy

Los derechos de los niños en el mundo digital

La Internet trae muchos beneficios para los niños, pero, al mismo tiempo, representa muchos riesgos. Promover estos beneficios y al mismo tiempo crear un entorno seguro y protegido requiere del equilibrio justo entre la protección de los niños contra los riesgos, y el respeto de sus derechos digitales, inclusive del derecho al acceso a la información y la libertad de expresión.

Consulte la Sección 3 para más información sobre los aspectos de seguridad del uso de Internet por parte de los niños.

La Convención sobre los Derechos del Niño (CDN)[28] de la ONU se considera como el pilar fundamental de los derechos de los niños. La CDN es uno de los tratados internacionales de derechos humanos más ratificado: al día de la fecha, todos los estados miembros de la ONU han ratificado la CDN, con la notable excepción de EE. UU.

La CDN reconoció por primera vez que los niños son personas que gozan de derechos humanos. La Convención está basada en cuatro principios fundamentales:

- Los niños deben estar libres de discriminación.
- Las políticas deberían estar basadas en el bienestar de los niños.
- Los niños deberían estar permitidos y motivados a desarrollar su máximo potencial.
- Los puntos de vista y las perspectivas de los niños son importantes y necesitan ser tomados en cuenta.

También aborda los derechos de los niños según tres amplias esferas: la disposición, la protección, y la promoción (o participación), comúnmente conocidas como las «tres p» en inglés.

Los desafíos

Enfoques proteccionistas

La protección en línea de los niños tiende a enfocarse en el aspecto protector del uso de la tecnología por parte de los niños. De hecho, muchos argumentan que la Internet y la tecnología incrementaron los riesgos para los niños, y que por lo tanto solamente pueden aprovechar los beneficios si esos riesgos son mitigados. Sin embargo, las políticas que se enfocan exclusivamente en los riesgos en línea pueden dejar de lado el potencial que tiene Internet para empoderar a los niños.

Un enfoque orientado hacia los derechos, basado en los derechos de los niños recogidos en los documentos jurídicos como la CDN, tiene como propósito maximizar las oportunidades que el mundo digital brinda a los niños y jóvenes, a la vez que los protege de los riesgos. Este enfoque se ve cada vez más favorecido por expertos gracias a que logra un equilibrio más justo entre los derechos digitales de los niños y la necesidad de protegerlos.

Aplicabilidad de la CDN en el mundo en línea

La CDN, adoptada de manera unánime en 1989, se formuló antes de la adopción masiva de Internet. ¿Aplica al mundo en línea? ¿Cómo?

La Resolución de 2012 del CDH de la ONU sobre la promoción, protección, y goce de los derechos humanos en Internet[29] concluyó el debate sobre que si los derechos humanos existentes aplican también en línea o si se necesita un nuevo conjunto de derechos para este entorno. Los expertos coinciden en que si bien este fue un logro significativo, se necesita tomar pasos más importantes con respecto a los derechos de los niños, quienes necesitan una protección especial.[30]

Particularmente, la CDN ofrece una guía de mutuo acuerdo sobre los principios e ideales para satisfacer los derechos de los niños fuera de línea, y puede también ofrecer la misma protección en línea, si se desarrolla de la manera adecuada. La CDN, por lo tanto, necesita traducirse a un claro conjunto de directrices.[31]

Si bien la CDN ordena a los gobiernos a actuar para el bienestar de los niños, también brinda un punto de partida desde el cual se pueden formular una variedad de políticas y medidas.

www.igbook.info/children

Los derechos de las personas con discapacidades[32]

Según las estimaciones de la Organización Mundial de la Salud (OMS), cerca de mil millones de personas en el mundo viven con algún tipo de discapacidad.[33] Este número crece debido al envejecimiento de la población; el surgimiento de nuevas enfermedades; afecciones crónicas; conflictos armados y violencia; pobreza y condiciones de vida insalubres; y la falta de conocimiento sobre la discapacidad, sus causas, su prevención y tratamiento.[34]

La Internet brinda nuevas posibilidades de inclusión social para las personas con discapacidades. Para maximizar las posibilidades tecnológicas de estas personas, se necesita el desarrollo de la gobernanza de Internet y el marco de políticas. El principal instrumento internacional en este campo es el de la Convención sobre los Derechos de las Personas con Discapacidad (CDPD de la ONU),[35] adoptada por la ONU en 2006, que establece los derechos que actualmente están en proceso de inclusión en la legislación nacional, lo que los hará aplicables.

La concientización de la necesidad de contar con soluciones tecnológicas que incluyan a las personas con discapacidades es cada vez mayor gracias al trabajo de organizaciones que instruyen y fomentan el apoyo a la comunidad de personas con discapacidad, como la Coalición Dinámica sobre Accesibilidad y Discapacidad del IGF,[36] el Capítulo de Discapacidad y Necesidades Especiales de la Internet Society, y el Centro Internacional de los Recursos de Internet para las Discapacidades.

Los desafíos de accesibilidad para las personas con discapacidades surgen de la brecha entre las capacidades que se requieren para la utilización de *hardware, software*, y contenido, y los recursos disponibles y las capacidades de una persona discapacitada. Para reducir esta brecha, las acciones políticas toman dos caminos:

- Incorporar estándares de accesibilidad en los requisitos para el diseño y el desarrollo de equipos, *software*, y contenido en línea.

- Fomentar la disponibilidad de los accesorios en *hardware* y *software* que aumenten o substituyan las capacidades funcionales de la persona con discapacidad.

En el campo de la gobernanza de Internet, el foco principal se encuentra en el contenido en línea y aplicaciones y su adecuación para el acceso y uso por parte de las personas con discapacidades. El W3C desarrolla los estándares internacionales en la accesibilidad de la web en el marco de la Iniciativa de Accesibilidad Web. A pesar de la existencia de estos estándares, muchas aplicaciones en línea aún no cumplen con ellos, debido a varios motivos, como la falta de conocimiento o la complejidad percibida y los altos costos.

www.igbook.info/disabilities

El género y los derechos humanos en línea

Los derechos de las mujeres en línea incluyen un amplio conjunto de temas relacionados con el acceso a Internet (por ejemplo, la violencia en línea), y la falta de acceso (por ejemplo, la pérdida de oportunidades en lo que respecta al acceso a la información, educación, comercio, y actividades políticas).

Históricamente, las niñas y mujeres han sufrido discriminación y grandes desigualdades en la educación (incluso en las especializaciones de las TIC), salud, bienestar social, participación política, y justicia. Muchas de estas desigualdades entre hombres y mujeres en el goce de derechos fundamentales se han replicado en línea. La violencia, la migración, los conflictos, y las crisis también han afectado el bienestar de las mujeres y su habilidad de satisfacer sus potenciales tanto en línea como fuera de línea, sufriendo importantes obstrucciones en sus vidas privadas.

Las mujeres representan más de la mitad de la población mundial, y aun así su participación en los procesos en los que interviene la tecnología es un área que aún necesita progresar. La protección de los derechos de las mujeres en línea es parte de un cambio sociocultural y profesional más grande que se centra en reducir la discriminación y los prejuicios en el ejercicio de los derechos, inclusive en el acceso a las oportunidades educacionales y económicas, el ejercicio de cargos públicos, y la igualdad salarial.

Aunque el acceso a Internet ha aumentado durante las últimas dos décadas, los patrones de uso generados crean oportunidades desiguales y generan importantes brechas en el empoderamiento de las niñas y mujeres en todo el mundo. Los datos de la UIT para el 2016 muestran que la grieta entre los géneros de los usuarios de Internet creció de un 11% en 2013 a un 12% en 2016 y la grieta más amplia (31%) continúa en los lugares en donde más se necesita el acceso: en los países menos desarrollados (PMD) del mundo. Los datos también señalan que la brecha de género regional más grande se da en África (23%) y la más pequeña en el continente americano (2%).[37]

Según un estudio de la Fundación WEB, incluso el acceso mejorado a teléfonos móviles no es suficiente para que las mujeres estén en línea, o «para lograr el empoderamiento de las mujeres por medio de la tecnología». El estudio indicó que aunque la mayoría de las mujeres y hombres poseen un teléfono, solamente el 37% de las mujeres tienen la posibilidad de acceder a Internet (aproximadamente la mitad de la cantidad de hombres en las mismas comunidades), y tienen una menor probabilidad (del 30 al 50%) de usar Internet para tomar oportunidades económicas o políticas. Además, mostró que el acceso está intrínsecamente ligado al nivel educacional: otro factor por considerar en la toma de medidas para producir cambios.[38]

Gracias a una mayor participación en línea, las mujeres se han podido desenvolver más en los ámbitos públicos y políticos, pero el hecho de que aprovechen por completo los beneficios de las TIC depende de la eliminación de una serie de barreras como la desigualdad del acceso y de la violencia contra las mujeres relacionada con la tecnología. Entre los actos de violencia cometidos a través de medios en línea se encuentran el ciberacoso, la vigilancia, y la vulneración de la privacidad, el acoso sexual, el uso no autorizado, y la manipulación de información personal, que incluye imágenes y videos. En la era de la conectividad generalizada, la creación de espacios en línea más seguros con la cooperación de los intermediarios de Internet toma el papel principal como el primer paso hacia el completo disfrute y desarrollo de los derechos humanos de las mujeres.

El informe de 2016 de la Relatora Especial de la ONU sobre la violencia contra la mujer, sus causas, y consecuencias tomó como un nuevo reto la violencia en línea contra la mujer. El informe indicó que «si bien el uso de la tecnología de la información y las comunicaciones ha contribuido al empoderamiento de las mujeres y las niñas, también ha generado diversas formas de violencia en línea». Instó a los estados y a los agentes no estatales a que «combatan la violencia en línea contra las mujeres y las niñas, al tiempo que respetan la libertad de expresión y la prohibición de la incitación a la violencia y al odio, de conformidad con lo dispuesto en el artículo 20 del Pacto Internacional de Derechos Civiles y Políticos».[39]

Los principales documentos internacionales para la protección de los derechos de las mujeres son la Convención sobre los Derechos Políticos de la Mujer de 1952 y la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW, por sus siglas en inglés). Tanto la ONU Mujeres como el CDH de la ONU trabajan de manera activa en varios aspectos de los derechos de las mujeres. Sin embargo, representa un reto incorporar las facetas en línea de las actividades de los órganos de derechos humanos de las mujeres inexistentes. Los grupos como la APC y la Coalición Dinámica sobre los Derechos de Género del IGF se han involucrado de manera activa en la defensa de los derechos en línea de las mujeres.

A medida que el movimiento de los derechos de las mujeres creció, se dio un paso para reconocer que esto es parte de una temática más amplia sobre los derechos de género, que también cubre los derechos de otras minorías de género. La temática de los derechos humanos sobre las mujeres y otras minorías de género, que incluye a la Comunidad de Lesbianas, Gays, Bisexuales, y personas Transgénero (LGBT), comprende la calidad de acceso a la información, las oportunidades profesionales, los procesos políticos globales, y otros derechos que son cruciales para los derechos humanos y gobernanza de Internet, y [40] deben ser estudiados y abordados en conformidad.

www.igbook.info/gender

NOTAS FINALES

[1] La *Carta de APC sobre derechos en Internet* incluye el acceso a Internet para todos; la libertad de expresión y asociación; el acceso al conocimiento; aprendizaje y creación compartidos – *software* gratuito y de código abierto y el desarrollo de la tecnología; la privacidad, vigilancia, y cifrado; la gobernanza de Internet; conciencia, protección, y efectividad de los derechos. Disponible en http://www.apc.org/en/node/5677 [accedido el 20 de octubre de 2016].

[2] Solon O (2015) Why the .sucks domain doesn't have to suck. *Bloomberg,* 19 de agosto. Disponible en http://www.bloomberg.com/news/articles/2015-08-19/why-the-sucks-domain-doesn-t-have-to-suck [accedido el 7 de marzo de 2016].

[3] ICANN (2016) Estatutos de la Corporación para la Asignación de Nombres y Números en Internet Disponible en https://www.icann.org/resources/pages/governance/bylaws-en [accedido el 7 de octubre de 2016].

[4] Borg-Psaila S (2011) Right to access the Internet: the countries and the laws that proclaim it. Disponible en http://www.diplomacy.edu/blog/right-access-Internet-countries-and-laws-proclaim-it [accedido el 20 de octubre de 2016].

[5] TJUE (2014) Sentencia del Tribunal de Justicia en el Caso C-131/12: Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Disponible en http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-131/12&td=ALL [accedido el 20 de octubre de 2016].

[6] Radu R and Chenou JM (2015) Data control and digital regulatory space(s): towards a new European approach. *Internet Policy Review* 4(2). Disponible en http://policyreview.info/articles/analysis/data-control-and-digital-regulatory-spaces-towards-new-european-approach [accedido el 20 de octubre de 2016].

[7] Bowcott O and Willsher K (2014) Google's French arm faces daily €1,000 fines over links to defamatory article. *The Guardian*, 13 de noviembre. Disponible en http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 [accedido el 20 de octubre de 2016].

[8] Unión Europea (2016) Reglamento (UE) del Parlamento Europeo y el Consejo del 27 de abril de 2016 sobre la protección de personas naturales con respecto al procesamiento de datos personales y el derecho al libre movimiento de dichos datos, por el que se deroga la Directiva 95/46/EC. Disponible en http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC [accedido el 14 de julio de 2016].

[9] Para obtener una revisión más detallada de las posibles implicaciones del derecho al olvido, lea a Keller D (2016) The new, worse 'right to be forgotten'. *Politico*, 27 de enero. Disponible en http://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/ [accedido el 14 de julio de 2016].

[10] Para una revisión de las razones para la restricción de las expresiones de opiniones extremas, así como también de argumentos para permitir una libertad de discurso más amplia, incluso con opiniones periféricas, consulte Heinze E (2014) Nineteen arguments for hate speech bans – and against them. Disponible en http://freespeechdebate.com/en/discuss/nineteen-arguments-for-hate-speech-bans-and-against-them/ [accedido el 12 de agosto de 2016].

[11] Poushter J (2015) 40% of millennials OK with limiting speech offensive to minorities. Disponible en http://www.pewresearch.org/fact-tank/2015/11/20/40-of-millennials-ok-with-limiting-speech-offensive-to-minorities/ [accedido el 12 de agosto de 2016].

[12] Naciones Unidas (1948) Declaración Universal de los Derechos Humanos. Disponible en http://www.un.org/en/documents/udhr/ [accedido el 20 de octubre de 2016].

[13] Freedom House (2016) Libertad en la Red 2016. Disponible en https://freedomhouse.org/report/freedom-net/freedom-net-2016 [accedido el 16 de november de 2016].

[14] Katitza Rodriguez, Directora Internacional de Derechos Civiles de la Electronic Frontier Foundation (EFF), aportó valiosos comentarios y contribuciones sobre este tema.

[15] UCLA (sin fecha) What is data mining? Disponible en http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm [accedido el 20 de octubre de 2016].

[16] Para conocer más detalles sobre la Ley Patriótica de EE. UU., visite el Electronic Privacy Information Centre (sin fecha) Ley Patriota de EE. UU. Disponible en https://epic.org/privacy/terrorism/hr3162.html [accedido el 20 de octubre de 2016].

[17] El foco de la privacidad y la preocupación relacionada con los sitios de redes sociales están bien ilustrados por el monitoreo atento y la presión que ejercen los defensores de los derechos civiles de los medios en Facebook. Para una revisión de una amplia gama de problemas de privacidad que emergen con el uso de esta plataforma, visite la Wikipedia (2012) *Criticism of Facebook*. Disponible en http://en.wikipedia.org/wiki/Criticism_of_Facebook [accedido el 20 de octubre de 2016].

[18] A modo de ejemplo, en agosto de 2016, el servicio de mensajería de Facebook, WhatsApp, cambió sus políticas de privacidad para que una vez que sus usuarios acepten los Términos y Condiciones de WhatsApp, automáticamente aceptaran compartir sus datos directamente con Facebook – incluso con el propósito de asignar publicidades. Optar por no compartir los datos directamente no parecía ser posible en el momento en que se introdujo el cambio, pero WhatsApp ofreció una posibilidad de no participación parcial con respecto al uso de los datos por parte de Facebook con propósitos de direccionamiento publicitario. Para obtener más detalles, consulte a Lamas N (2016) WhatsApp to share user data with Facebook for targeting – here's how to opt out. *Techcrunch*, 25 de agosto. Disponible en https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/ [accedido el 20 de octubre de 2016].

[19] Para una revisión de las vulneraciones de la privacidad más importantes en el tiempo, lea a Lord N (2016) The History of Data Breaches. *Digital Guardian,* 12 de octubre. Disponible en https://digitalguardian.com/blog/history-data-breaches [accedido el 20 de octubre de 2016].

[20] *The Economist* (2004) *Move over, Big Brother.* 2 de diciembre. Disponible en http://www.economist.com/node/3422918 [accedido el 30 de octubre de 2016].

[21] Gov.track.us (sin fecha) Ley de Prevención contra el Video Voyerismo. Disponible en https://www.govtrack.us/congress/bills/108/s1301/text [accedido el 20 de octubre de 2016].

[22] Consejo de Europa (sin fecha) Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal. Disponible en http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 [accedido el 20 de octubre de 2016].

[23] Unión Europea (1995) Directiva 95/46/EC del Parlamento Europeo y del Consejo del 24 de octubre de 1995 sobre la protección de las personas con respecto al tratamiento de datos de carácter personal y a la libre circulación de esos datos. Disponible en http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046 [accedido el 20 de octubre de 2016].

[24] Unión Europea (2016) Reglamento (EU) 2016/679 del Parlamento Europeo y del Consejo de octubre del 27 de abril de 2016 sobre 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. Disponible en http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 [accedido el 27 de agosto de 2016].

[25] OCDE (2013) Directrices actualizadas de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. Disponible en http://www.oecd.org/sti/ieconomy/privacy.htm [accedido el 30 de octubre de 2016].

[26] TJUE (2015) Sentencia del Tribunal en el Caso C-362/14: Maximilliam Schrems vs Data Protection Commissioner. Disponible en http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2015 [accedido el 21 de octubre de 2016].

[27] Comisión Europea (2016) Decisión de Ejecución de la Comisión sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. Disponible en http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2016_207_R_0001 [accedido el 21 de octubre de 2016].

[28] Naciones Unidas (1989) Convención sobre los Derechos del Niño (1989). Disponible en http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx [accedido el 21 de octubre de 2016].

[29] Consejo de Derechos Humanos de la ONU (2012) Resolución A/HRC/20/L.13 sobre la promoción, la protección y el goce de los derechos humanos en Internet. Disponible en http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280 [accedido el 21 de octubre de 2016].

[30] Livingstone S and Bulgar M (2014) A global research agenda for children's rights in the digital age. *Journal of Children and Media* 8(4). Disponible en http://www.lse.ac.uk/media@lse/WhosWho/AcademicStaff/SoniaLivingstone/pdf/Livingstone-&-Bulger-JOCAM-A-global-research-agenda-for-childrens-rights-in-the-digital-age.pdf [accedido el 18 de agosto de 2016].

[31] Para un análisis de cómo aplican los artículos de la CDN al entorno digital, diríjase a: Livingstone S and Bulgar M (2014), *ibíd,* y Livingstone S y O'Neill B (2014). Children's rights online: Challenges, dilemmas and emerging directions. In S. van der Hof *et al.* (Eds), *Minding minors wandering the web: Regulating online child safety.* Berlín: Springer.

[32] Jorge Plano, Profesor en la Universidad Tecnológica Nacional de Buenos Aires, aportó valiosos comentarios y contribuciones en esta sección.

[33] Organización Mundial de la Salud (2015) Discapacidad y salud. Nota informativa Nº 352. Disponible en http://www.who.int/mediacentre/factsheets/fs352/en/ [accedido el 21 de octubre de 2016].

[34] Disabled World (sin fecha) *Disability Statistics: Facts & Statistics on Disabilities & Disability Issues*. Disponible en http://www.disabled-world.com/disability/statistics/ [accedido el 21 de octubre de 2016].

[35] Naciones Unidas (2006) Convención sobre los Derechos Humanos de las Personas con Discapacidad. Disponible en http://www.un.org/disabilities/convention/conventionfull.shtml [accedido el 21 de octubre de 2016].

[36] La Coalición Dinámica sobre Accesibilidad y Discapacidad del IGF desarrolló un conjunto de directrices de accesibilidad, que están disponibles en http://www.intgovforum.org/cms/dynamiccoalitions/80-accessibility-and-disability#documents [accedido el 10 de agosto de 2016].

[37] UIT (2016) Hechos y cifras de las TIC 2016. Disponible en http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf [accedido el 21 de octubre de 2016].

[38] Fundación WEB (2015) Women's Rights Online: Translating Access into Empowerment. Disponible en http://webfoundation.org/about/research/womens-rights-online-2015/ [accedido el 12 de agosto de 2016].

[39] Naciones Unidas (2016) Reporte de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias (2016) Informe. Disponible en http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/42 [accedido el 7 de noviembre del 2016].

Sección 9

ACTORES EN LA GOBERNANZA DE INTERNET

Actores en la gobernanza de Internet

La gobernanza de Internet involucra a una gran variedad de actores o partes interesadas (como se las suele llamar), como los gobiernos nacionales, las organizaciones internacionales, el sector comercial, la sociedad civil, y las comunidades académicas y técnicas (como se especifica en el párrafo 49 de la Declaración de Principios de la CMSI de 2003 y en los párrafos 35 y 36 de la Agenda de Túnez para la Sociedad de la Información de la CMSI de 2005. Aunque la condición que ejercen las múltiples partes interesadas se adopta como un principio de la gobernanza en los documentos de la CMSI, el principal debate gira en torno al rol específico y las responsabilidades de los actores, haciendo especial foco en la relación entre los actores estatales y los no estatales en las diferentes áreas de la gobernanza de Internet.

La mayoría de los actores de la gobernanza de Internet se enfrentan con el desafío de lidiar con la alta complejidad de este campo, que se caracteriza por el carácter multidisciplinario de sus asuntos, que son de naturaleza tecnológica, legal, económica, de derechos humanos, y sociocultural, entre otras. Además, los asuntos de la gobernanza de Internet se abordan desde distintos niveles de políticas: local, nacional, regional, y global. Esta sección proporciona una revisión de los principales actores de la gobernanza de Internet, y un resumen de sus correspondientes posiciones.

¿Cuál es la principal diferencia conceptual entre la gobernanza de Internet y otros procesos de políticas globales?

En la gobernanza de Internet, los gobiernos tuvieron que entrar en un régimen no gubernamental ya existente, formado en torno a la IETF, la Internet Society, y ICANN. En otras áreas de políticas (por ejemplo, las del cambio climático, el comercio, la migración), esto sucedió en la otra dirección. El espacio de políticas intergubernamentales se ha estado abriendo de manera gradual a los actores no gubernamentales. Desde la CMSI de 2003, momento en el que varios gobiernos empezaron a entrar en la escena de la gobernanza de Internet, el principal desafío ha sido el de sincronizar el régimen no gubernamental existente de la gobernanza de Internet con el tradicional y diplomático. Esta convergencia no solo ha disparado las principales controversias acerca de los roles de los gobiernos y otros actores en la gobernanza de Internet, sino que también ha creado oportunidades para convertir la elaboración de políticas en un mecanismo más inclusivo y efectivo.

Gobiernos

La Internet, como la tecnología que define a la era moderna, afecta la geopolítica de los estados (centrados en el asunto de la seguridad nacional), y, cada vez más, sus geoeconomías (que se definen como la promoción de intereses nacionales a través de medios económicos). La Internet también crea altos niveles de interdependencia económica y social, lo que provoca una necesidad de identificar soluciones de políticas por medio de las

negociaciones y la cooperación. La gobernanza de Internet se introdujo en la agenda diplomática global en 2003-2005, durante el proceso de la CMSI. Desde ese momento, varios gobiernos han intentado comprender este complejo campo de políticas.

La relevancia crucial de la Internet para las sociedades nacionales en todo el mundo ha ejercido una presión adicional a los gobiernos para desarrollar una gobernanza de Internet efectiva a nivel nacional y para involucrarse en esfuerzos de diplomacia de Internet para proteger sus intereses en el ámbito digital.

Los esfuerzos internacionales de los gobiernos se han canalizado en dos direcciones principales. En primer lugar, los gobiernos tratan con la Internet, como una nueva cuestión de política, en una amplia gama de espacios, desde entidades de múltiples partes, como ICANN y el IGF, hasta las multilaterales, como la UIT y el GGE de la ONU (vea, por ejemplo, la Cuadro 3, que muestra la participación de los gobiernos en el GGE). En segundo lugar, los gobiernos tienen que ocuparse de los aspectos digitales de las cuestiones políticas tradicionales, como el comercio (en el contexto de la OMC), la salud (OMS), y el trabajo (OIT).

Incluso para países grandes y ricos, los asuntos relacionados con la gobernanza de Internet han causado numerosos desafíos, tales como la gestión de su naturaleza multidisciplinaria (es decir, los aspectos tecnológicos, económicos, y sociales) y la participación de una gran variedad de actores. Estos gobiernos han tenido que realizar diferentes actividades al mismo tiempo: capacitar a los funcionarios, desarrollar políticas, y participar de manera activa en las diversas reuniones internacionales sobre Internet.

Coordinación nacional

En 2003, en los comienzos del proceso de la CMSI, la mayoría de los países abordaba los temas relacionados con la gobernanza de Internet por medio de ministerios de telecomunicaciones y autoridades regulatorias – por lo general aquellas que habían estado a cargo de las relaciones con la UIT, la principal organización internacional que se encarga de los asuntos de las telecomunicaciones. De manera gradual, con el creciente impacto de la Internet en la estructura política, social, y económica de la sociedad moderna, otros departamentos gubernamentales comenzaron a involucrarse en la gobernanza de Internet: asuntos exteriores, cultura, medios, y justicia.

El desafío más importante para muchos gobiernos ha sido desarrollar una estrategia para reunir y coordinar de manera efectiva el apoyo de actores no estatales, como las universidades, las compañías privadas, y las ONG, que generalmente cuentan con la experticia necesaria para tratar asuntos relacionados con la gobernanza de Internet. En los años posteriores a la CMSI de 2003, la mayoría de los países G20 grandes y medianos pudieron desarrollar la capacidad institucional necesaria para seguir las negociaciones globales de la gobernanza de Internet. Algunos de ellos, como Brasil, han desarrollado estructuras nacionales innovadoras con el propósito de seguir los debates de la gobernanza de Internet. Estas estructuras incluyen: ministerios de telecomunicaciones, el servicio diplomático, el sector comercial, la sociedad civil, y el sector académico.[1] La India, Indonesia, y Kenia son otros de los ejemplos de países que han creado una cooperación de múltiples partes interesadas a nivel nacional. Muchos países usan iniciativas nacionales del IGF para vincularse con los diferentes grupos de partes interesadas en la gobernanza de Internet y en los procesos de políticas globales. En octubre de 2016, la Secretaría del IGF global reconoció 47 iniciativas nacionales.[2]

Coherencia de políticas

Dada la naturaleza multidisciplinaria de la gobernanza de Internet y la gran diversidad de actores y foros de políticas, lograr la coherencia de políticas es todo un reto. Por ejemplo, el asunto de la privacidad y la protección de datos se aborda desde las perspectivas de derechos humanos, comercio, normalización, y seguridad, entre otras; pero a menudo estas perspectivas (Figura 26) encuentran escasa coordinación entre las políticas y los grupos de expertos que abordan cada una de ellas. Lograr la coherencia de políticas en el campo de la gobernanza de Internet requiere una forma flexible de coordinación de estas, incluida una comunicación horizontal entre los diferentes ministerios, el sector comercial, y otros actores.

Además del desafío de su administración, lograr una coherencia de políticas está por lo general limitado por la existencia de intereses competitivos de políticas. Esto es más evidente en países con economías de Internet bien desarrolladas y diversificadas. Por ejemplo, al comienzo del debate sobre la neutralidad de la red, varios reguladores de distintos países intentaron lograr un equilibrio entre la industria de Internet, que apoyaba la neutralidad de la red; y los sectores de las telecomunicaciones y del entretenimiento, que consideraban que la neutralidad de la red era un obstáculo para desarrollar un nuevo modelo de negocio basado en, por ejemplo, una Internet más veloz para la entrega del contenido multimedia.

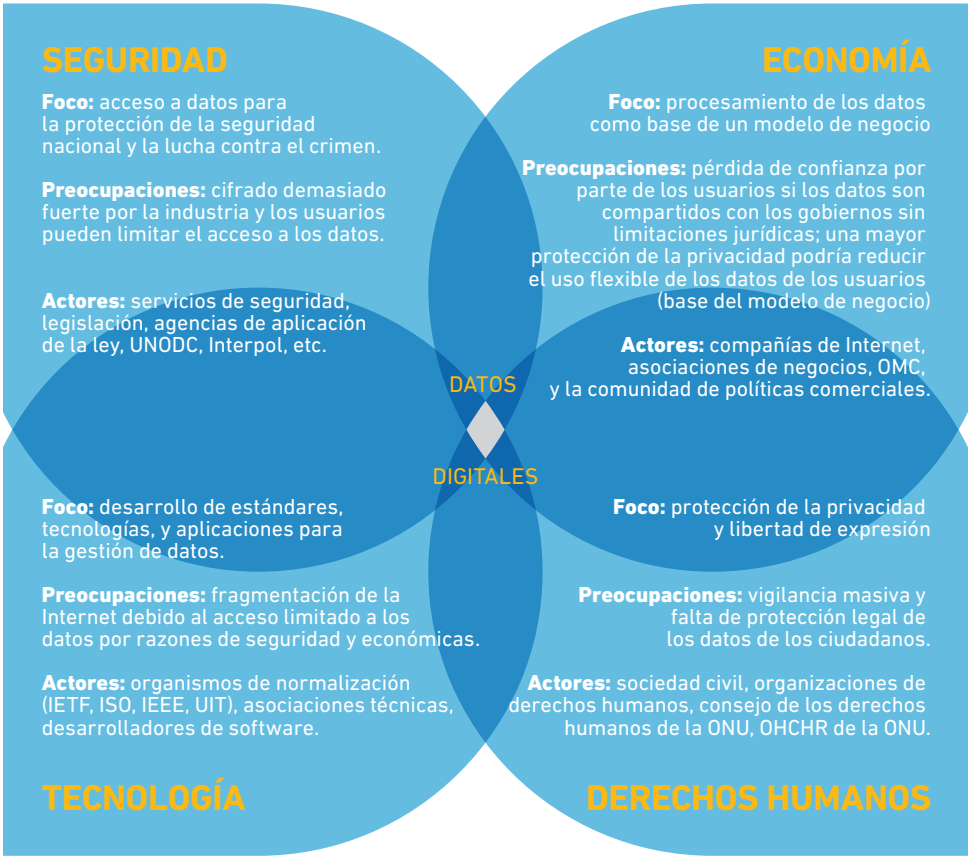

Figura 26. Convergencia de los silos de políticas en el ámbito digital

Rol de las misiones permanentes sobre la gobernanza de Internet con base en Ginebra

Para varios gobiernos, sus misiones permanentes en Ginebra han sido jugadores de gran importancia, casi vitales, en los procesos de la CMSI y la gobernanza de Internet. Muchas de las actividades relacionadas con la primera etapa de la gobernanza de Internet se llevaron a cabo en Ginebra, sede central de la UIT, que tomó un papel protagónico en los procesos de la CMSI. La primera fase de la CMSI se llevó a cabo en Ginebra en 2003, lugar en donde se llevaron a cabo todas las reuniones preliminares (excepto una), manteniendo las misiones permanentes basadas allí involucradas de manera directa. Actualmente, la Secretaría del IGF tiene base en Ginebra y muchas de las reuniones preliminares del IGF se organizan allí.

Geoestrategia de cableado e (in)coherencia de políticas

La Entente Cordiale[3] se estableció en 1904. Al consolidar una cooperación cercana con Alemania, sin embargo, el ministerio telegráfico de Francia no siguió la política exterior del país sobre la preferencia de las relaciones con Gran Bretaña. La principal razón de esto fue para reducir la dominancia británica en la geoestrategia de cableado global al instalar nuevos cableados para telégrafos en asociación con Alemania. En 1915, el historiador francés Charles Lesage hizo el siguiente comentario acerca de esta (in)coherencia de políticas: «El desacuerdo prolongado entre los principios generales de la diplomacia francesa y los procedimientos de las políticas telegráficas, en mi opinión, son el resultado de que en este país, cada ministerio tiene su propia política exterior: el Ministerio de Relaciones Exteriores tiene una, el Ministerio de Finanzas, otra… La Administración de Correos y Telégrafos también cuenta con, de vez en cuando, una política exterior; y así sucedió en los últimos años, sin mostrarse completamente hostil frente Inglaterra, demostró una fuerte inclinación hacia Alemania».[4]

Para los países grandes y desarrollados, las misiones permanentes en Ginebra han formado parte de la amplia red de instituciones e individuos que abordan las cuestiones de los procesos de la CMSI y la gobernanza de Internet. Para los países pequeños y en vías de desarrollo, estas misiones han sido los principales (y en algunos casos los únicos) jugadores en estos procesos. Algunas cuestiones de la gobernanza de Internet se han agregado a la agenda de las pequeñas y sobreexigidas misiones de los países en vías de desarrollo. En muchos casos, los mismos diplomáticos deben tomar la responsabilidad de tareas asociadas con los procesos de la gobernanza de Internet, junto con otros asuntos, como los derechos humanos, la salud, el comercio, y el trabajo.

Posición de los gobiernos nacionales

Estados Unidos

La Internet fue creada como parte de un proyecto científico patrocinado por el gobierno de los Estados Unidos. Desde su nacimiento hasta el día de hoy, el gobierno de EE.UU. ha estado ligado a la gobernanza de Internet por medio de diferentes departamentos y agencias: en un primer momento, el Departamento de Defensa; y más tarde, la Fundación

Nacional para la Ciencia (NSF, por sus siglas en inglés). El último fue el Departamento de Comercio. La FCC también ha jugado un papel importante en la creación de un marco regulatorio para Internet.

Una de las participaciones constantes del gobierno de EE.UU. ha sido su enfoque no intervencionista, generalmente conocido como «custodio a distancia». Plantea un marco pero deja a la gobernanza de Internet en manos de aquellos que trabajan de manera directa con ella, principalmente la comunidad técnica. Sin embargo, el gobierno estadounidense ha intervenido más directamente en algunas ocasiones, como ocurrió a mediados de la década de 1990, cuando el proyecto sin fines de lucro CORE (Consejo de Registradores) podría haber trasladado el servidor raíz y la gestión de la infraestructura principal de Internet desde EE.UU. hasta Ginebra.[5] El proceso fue detenido a causa de una nota diplomática famosa (por lo menos en la historia de la Internet) enviada por la Secretaria de Estado de EE.UU., Madeleine Albright, a la Secretaría General de la UIT.[6] Al mismo tiempo que intentó detener la iniciativa CORE, el gobierno estadounidense inició una serie de conferencias que resultaron en el establecimiento de ICANN, en 1998. El gobierno de EE.UU. le confirió a ICANN el rol de llevar a cabo las funciones de la IANA: coordinar los sistemas de identificadores únicos de Internet (principalmente el DNS, y los números IP). El gobierno de EE.UU. mantuvo el rol de la administración de las funciones de la IANA hasta octubre de 2016, momento en el cual este rol fue transferido a la comunidad global de Internet.

El hecho de que EE.UU. goce de un espacio en línea bien desarrollado y una industria de la Internet envidiable hace que sea un país particularmente propenso a los ataques a la ciberseguridad. En consecuencia, la diplomacia estadounidense tiene un papel muy activo en las negociaciones internacionales sobre la ciberseguridad. Los Estados Unidos apoyan la idea de que las normas de seguridad existentes, como el derecho a la autodefensa, deberían también aplicar a Internet; y se opone a la adopción de un tratado global sobre ciberseguridad. Sin embargo, es una de las partes en una gran variedad de acuerdos bilaterales y regionales sobre esta cuestión. Los Estados Unidos abordan el tema de la ciberdelincuencia internacional mediante el Convenio sobre la Ciberdelincuencia del CdE, así como también mediante acuerdos bilaterales, incluidos los MLAT. También apoya el desarrollo de estructuras de ciberseguridad, al establecer o fortalecer, por ejemplo, los CERT existentes.

En lo que respecta a los asuntos económicos, EE.UU. está a favor del libre flujo de datos y del libre comercio con servicios digitales. El libre comercio en línea es promovido por la OMC y por medio de varios acuerdos comerciales regionales y bilaterales. La industria estadounidense de Internet es la principal beneficiada del libre comercio, siendo el flujo libre de datos un aspecto muy importante. El país se opone a las cargas fiscales para las transacciones en línea.

Unión Europea

La Unión Europea tiene una mezcla de poderes digitales duros y blandos para forjar una conciliación acerca de la gobernanza de Internet. Su poder duro se basa en la atracción de un mercado de 500 millones de personas con alta penetración de Internet (79,3% en 2015)[7] y poder adquisitivo también. Así como lo demuestra la concentración de presión de la industria de la Internet en Bruselas, este poder duro realmente importa. Por medio de una serie de negociaciones con la UE sobre asuntos antimonopólicos y la protección de datos, Google y Facebook, entre otros, negocian con el resto del mundo (los acuerdos de la UE con la industria de la Internet a menudo inspiran a otros países y regiones a reaccionar de

manera similar). En una situación en donde, por ejemplo, Google tiene un porcentaje del 90% del mercado de búsquedas en línea en el Área Económica Europea, la UE se posiciona como la principal entidad que podría asegurar que la alta penetración al mercado europeo por parte de Google no sea indebida a través de prácticas que incluyan el abuso de la posición dominante de la compañía en el mercado.[8]

Su poder blando se basa en una especie de diplomacia aikido digital de transformar las debilidades en fortalezas. Aunque la UE no cuenta con una industria de Internet fuerte, esta debilidad podría, paradójicamente, convertirse en una fortaleza en la gobernanza de Internet.

A saber, al no tener la necesidad de proteger los intereses económicos de la industria de Internet, la UE posee mayor libertad para promover y proteger los intereses públicos (derechos de los usuarios, inclusión, diversidad de contenido). De esta manera, la UE puede convertirse en la guardiana de los «usuarios de Internet», y la promotora de un entorno que habilite el crecimiento de la industria de Internet de la UE. La Unión podría lograr tanto los objetivos éticos como los estratégicos, cosa que no ocurre en las políticas internacionales.

Ha comenzado a emerger un enfoque de la UE que se basa en formar diferentes alianzas en torno a distintas cuestiones. En la CMTI-12, EE.UU. encontró el apoyo de Europa. Con respecto a la protección de datos y la privacidad, la postura de la UE se asemeja a la de los países latinoamericanos. Suiza y Noruega toman posiciones similares a la de la UE en lo que respecta a la mayoría de los asuntos de la gobernanza de Internet.

En los años venideros, la postura de la UE en la gobernanza de Internet será moldeada aún más con la creación del Mercado Único Digital para la UE, especialmente en áreas como la tributación, la protección de los consumidores, y el libre flujo de datos.

Los estados miembros de la UE han estado poniendo especial atención a los temas relacionados con la gobernanza de Internet, desarrollando sus áreas nicho. Alemania y Austria tienen sus preocupaciones acerca de la privacidad y la protección de datos, por lo que desenvuelven un papel protagonista en los debates sobre la protección de la privacidad en línea dentro de la UE y el sistema de la ONU.

Estonia es un actor de políticas digitales muy dinámico. Luego del ataque DDoS en 2007, que afectó gravemente a la Internet a nivel nacional, Estonia se convirtió en un jugador realmente activo en el campo de la ciberseguridad. Cuenta con el Centro de Excelencia de la OTAN de Ciberdefensa Cooperativa así como también con la Conferencia sobre el Ciberconflicto, un evento muy importante sobre la ciberseguridad que se lleva a cabo anualmente desde 2010.

Rumania se ha estado especializando en el campo de la lucha contra la ciberdelincuencia. Cuenta con la Oficina de Programas sobre la Ciberdelincuencia del CdE, cuyo objetivo es asistir a los países para fortalecer sus sistemas judiciales penales y su capacidad de responder ante los desafíos presentados por la ciberdelincuencia, sobre la base de los estándares del Convenio sobre la Ciberdelincuencia.

Los Países Bajos son la sede del Foro Global de Experticia Cibernética y un gran número de iniciativas en el campo de la ciberseguridad.

China

China es un jugador importante en la gobernanza de Internet, ya que es el país con el mayor número de usuarios de Internet en el mundo (más de 700 millones) y su industria de Internet va en rápido crecimiento (cuatro de cada diez compañías de Internet importantes son chinas). China ha estado equilibrando su postura en las políticas digitales entre un enfoque impulsado por la economía para lograr comunicaciones de Internet ilimitadas que vayan más allá de las fronteras nacionales, y un enfoque de cibersoberanía impulsado por la política para las actividades relacionadas con la Internet a nivel nacional.

Desde la perspectiva económica, la Internet global es de vital interés para la economía china, que se basa en las exportaciones. Algunas compañías chinas usan la Internet como la infraestructura de la información para sus operaciones de negocios en todo el mundo. Alibaba, la plataforma de Internet más importante para los negocios de China, actualmente cuenta con el volumen más alto de transacciones de comercio electrónico a nivel mundial. El propietario de Alibaba, Jack Ma, ha estado solicitando la creación de una Plataforma Electrónica de Comercio Global, con el objetivo de asistir a PyMEs en la participación del comercio digital global.[9] En la reunión G20 en Hangzhou, en septiembre de 2016, China promovió fervientemente la economía y la innovación digitales.

Desde la perspectiva política, la protección de la soberanía como la piedra angular de la política exterior china se ve reflejada también en el ciberespacio. El presidente chino Xi definió a la cibersoberanía en la Conferencia Mundial de Internet de 2015 como «el derecho que los países tienen a elegir de forma independiente cómo avanzar por el camino del desarrollo cibernético, así como de emitir sus propios reglamentos y políticas públicas de Internet, y de participar en la gobernanza del ciberespacio internacional de manera equitativa».[10] De acuerdo con el enfoque de la cibersoberanía, la Internet debe cumplir con las leyes, costumbres, y la gobernanza del espacio físico delimitado por los límites nacionales.

China alcanzó un alto nivel de cibersoberanía al restringir el acceso al mercado chino por parte de las compañías de Internet extranjeras (Facebook, Google, Twitter), y, en cambio, fomentar la prestación de servicios similares por medio de compañías chinas como: Baidu (equivalente de Google), Sina Weibo (equivalente de Twitter), Renren (equivalente de Facebook), Youku (equivalente de YouTube). La mayor parte de los datos que pertenecen a los individuos o instituciones chinos se almacenan en servidores en China. Posiciones críticas al enfoque de la cibersoberanía de China tienen que ver con el filtrado del contenido en línea que el gobierno considera inapropiado para la difusión pública.

En el espacio de políticas digitales globales, China generalmente apoya un enfoque multilateral. Sin embargo, también participa de manera activa en procesos y organismos de múltiples partes involucradas, como ICANN y la IETF. En sus esfuerzos por participar de manera más activa en las políticas digitales internacionales, China ha sido la sede de las Conferencias Mundiales de Internet, que se llevan a cabo anualmente desde el 2014.

En los años por venir, la política digital exterior de China apoyará la creación de la Ruta de Seda Digital, destinada a incrementar la conectividad digital entre Asia y Europa. La Ruta de Seda Digital formará parte de un proyecto más amplio – Un Cinturón, Una Ruta – que une a China y a Europa mediante numerosas conexiones terrestres y marítimas.

Brasil

Brasil ha sido uno de los países más activos en lo que respecta a las políticas digitales globales, y es el mercado de Internet más grande de América Latina. Brasil, como país democrático y en vías de desarrollo pero con un espacio digital pujante, tiene un gran potencial para facilitar un término medio entre los dos bandos en el debate sobre la gobernanza de Internet (el intergubernamental y el no gubernamental). Este papel se volvió evidente tras las revelaciones de Snowden, momento en el que Brasil tomó fuertes acciones diplomáticas. La presidente brasileña Dilma Rousseff, en su discurso en el 68° periodo de sesiones de la AGONU pidió que la ONU desempeñe un rol de liderazgo en todos los esfuerzos destinados a regular la conducta de los Estados en lo que se refiere a estas tecnologías. Además, definió a la vigilancia como una brecha en la ley internacional y una «falta de respeto a la soberanía nacional» de su país.[11] Cuando parecía que Brasil insistía en un enfoque intergubernamental, Rousseff se volvió al centro del espectro de la política al proponer la coorganización de una reunión de NETmundial, que tuviera el objetivo de llevar a cabo mayores desarrollos en el modelo de gobernanza de Internet de múltiples partes interesadas. Brasil tuvo que tomar un papel complejo, en el que su finalidad principal fue asegurar un resultado exitoso (aunque no vinculante) de la reunión.[12]

Brasil es muy activo en numerosos procesos de política digital. El país acogió dos de las 10 reuniones del IGF. Ha desempeñado un papel de liderazgo en las negociaciones de WSIS + 10. Junto con Alemania, Brasil ha sido un fuerte promotor de la protección internacional de la privacidad en línea.

India

La India es otro jugador prominente en la política digital. Este país cuenta con una base de usuarios de Internet amplia y una industria de Internet avanzada. Sin embargo, también enfrenta desafíos relacionados con brindar acceso a su población numerosa. Las complejas políticas de gobernanza de Internet de la India reflejan la complejidad de su elaboración de políticas digitales nacionales. Este país cuenta con uno de los escenarios de sociedad civil más diversos y dinámicos de la gobernanza de Internet global. En el pasado, el gobierno de la India solía inclinarse hacia el enfoque intergubernamental con respecto a la gobernanza de Internet, mientras que el sector comercial se ha mostrado más defensor del enfoque no gubernamental. Esta dicotomía impulsó unas maniobras sorprendentes. Por ejemplo, la India propuso la creación de un Comité relacionado con las Políticas de Internet de la ONU, para lograr la supervisión intergubernamental de los CIR. Se trasladó al otro lado del espectro de las políticas de Internet en la CMTI-12 cuando se puso del lado de los países desarrollados al no firmar las modificaciones del RTI, algo que la mayoría de los países en vías de desarrollo sí hizo. La administración actual de la India apoya el modelo de gobernanza de Internet de múltiples partes interesadas, como se reiteró durante la reunión N° 57 de ICANN, llevada a cabo en la India en noviembre de 2016.[13]

Rusia

Rusia ha sido el propulsor más expresivo y consistente de un enfoque multilateral de la gobernanza de Internet, con un papel de liderazgo para los gobiernos en el abordaje de temas de política pública relacionados con Internet. En particular, Rusia ha promovido el rol de la UIT en el campo de la gobernanza de Internet. En el ámbito de la ciberseguridad internacional, Rusia tomó primeros pasos en 1998, al presentar una propuesta que luego

se convertiría en la primera resolución de la AGONU relativa a las TIC y a la seguridad.[14] Desde ese año, esta resolución se ha repetido anualmente, preparando el camino para abordar la ciberseguridad mediante el trabajo del primer comité de la AGONU, y, recientemente, el GGE de la ONU.[15] Junto con China, Kazajistán, Tayikistán, y Uzbekistán, Rusia también busca la cibercooperación en otros espacios institucionales. De manera notable, en el marco de la OCS, existe un acuerdo internacional sobre la seguridad de la información de 2009.

En septiembre de 2015, Rusia introdujo una regulación de localización de datos, que requería que las compañías de Internet almacenaran los datos de los usuarios rusos dentro de los límites nacionales. Esta ley puede forzar a las compañías de Internet más importantes, como Facebook, Twitter, Google, y LinkedIn a colocar sus servidores en Rusia, o que se arriesguen a que sus servicios sean bloqueados dentro del territorio ruso.

Kenia

Kenia es uno de los jugadores más dinámicos en la gobernanza de Internet. Presenta un panorama activo de múltiples partes interesadas, un IGF nacional, y una participación activa por parte de la sociedad civil, la comunidad comercial, y el sector académico en las iniciativas de la gobernanza de Internet lideradas por el gobierno.

Uno de los mayores éxitos de Kenia ha sido el del sistema de pago MPesa, que ha proporcionado a millones de sujetos el acceso a servicios financieros. Este sistema impulsó enormemente la industria nacional de Internet, a la vez que se ha exportado a otros países.

Kenia tiene una participación activa en los procesos de políticas digitales de África y el mundo. Fue sede del encuentro anual del IGF en 2011. Además, representantes del gobierno de Kenia, de la comunidad comercial, y de la sociedad civil forman parte de los participantes más activos en la UIT, ICANN, el IGF, y la AGONU, entre otros.

Indonesia

Indonesia ha sido protagonista de un rápido crecimiento de la Internet, con un alcance de 53 millones de usuarios en 2016. Para Indonesia, como país-archipiélago, la Internet es una infraestructura crítica, que conecta a más de 6000 islas habitadas.

Indonesia cuenta con un IGF nacional, que reúne a los representantes de las instituciones gubernamentales, entidades comerciales, el sector académico, y la sociedad civil. En el ámbito de la seguridad, la principal preocupación del país está relacionada con el uso de la Internet por parte de grupos terroristas. Desde la perspectiva de la economía, Indonesia ha considerado la implementación de un impuesto especial para Google y otras compañías de Internet. En el campo de la privacidad y la protección de datos, Indonesia adoptó el derecho al olvido. Además del concepto europeo sobre el derecho al olvido (es decir, permitir la desindexación de contenido específico de los resultados de motores de búsqueda), Indonesia también brinda la posibilidad de borrar contenido irrelevante de sitios web.

Indonesia ha mostrado una participación activa en la política digital internacional. En 2013, fue sede del encuentro anual del IGF. También ha participado de manera activa en actividades de la UIT, ICANN, el IGF, y el GGE de la ONU.

Cuadro 3: Resumen de miembros de los cinco GGE de la ONU creados desde 2004

Países \ Año	2004–2005	2009–2010	2012–2013	2014–2015	2016–2017
Argentina			■		
Australia			■		■
Bielorrusia	■	■	■	■	
Botsuana					■
Brasil	■	■		■	■
Canadá			■		■
China	■	■	■	■	■
Colombia				■	
Cuba					■
Egipto			■	■	■
Estonia		■	■	■	■
Finlandia					■
Francia	■	■	■	■	■
Alemania	■	■	■	■	■
Ghana				■	
India	■	■	■		■
Indonesia			■		■
Israel		■		■	
Italia		■			
Japón			■	■	■
Jordania	■				
Kazajistán					■
Kenia				■	■
Malasia	■			■	
Mali	■				
México	■			■	■
Países Bajos					■
Pakistán				■	
Catar		■			
República de Corea	■	■		■	■
Federación Rusa	■	■	■	■	■
Senegal					■
Serbia					■
Sudáfrica	■	■			
España				■	
Suiza					■
Estados Unidos de América	■	■	■	■	■
Reino Unido	■	■	■	■	■

Suiza

Suiza ha tenido un rol pionero en el desarrollo del ecosistema global de la gobernanza de Internet, desde el primer evento significativo, que se llevó a cabo en Ginebra en la fase de la CMSI de 2003. El diplomático suizo Markus Kummer lideró el GTGI y, posteriormente, la Secretaría del IGF (hasta el 2010). Desde 2014, el GAC de ICANN ha estado presidido por Thomas Schneider, un funcionario de la Oficina Federal de Comunicaciones de Suiza.

En el campo de la ciberseguridad, Suiza ha contribuido ampliamente al desarrollo de las CBM para el ciberespacio. Hoy en día, Suiza es miembro del GGE de la ONU (2016-2017).

En el ámbito de los derechos humanos, Suiza es uno de los países que apoyan activamente la protección de la privacidad en el espacio en línea, a través de la ONU y otros mecanismos internacionales.

Estados pequeños

La complejidad de los asuntos y las dinámicas de las actividades hicieron que fuera casi imposible para algunos países pequeños, en particular los que están en vías de desarrollo, seguir los procesos de políticas de la gobernanza de Internet. Como resultado, algunos estados pequeños han apoyado la estructura de «ventanilla única» para los temas

Gobernanza de Internet – un enfoque de geometría variable

La gobernanza de Internet requiere la participación de diferentes partes interesadas, que difieren en muchos aspectos, como la capacidad jurídica internacional, el interés en asuntos particulares de la gobernanza de Internet, y la experticia disponible. Tal variedad puede adaptarse por medio del uso del enfoque de geometría variable, que se especifica en el párrafo 49 de la Declaración de Principios de la CMSI,[17] que estipula los siguientes roles para las principales partes interesadas:

- Estados – «autoridad de políticas […] para las cuestiones de política pública internacional de Internet» (incluidos los aspectos internacionales).
- El sector privado – «desarrollo de Internet, en los campos técnico y económico».
- Sociedad civil – «un importante papel en asuntos relacionados con Internet, especialmente a nivel comunitario».
- Organizaciones intergubernamentales – «coordinación de las cuestiones de políticas públicas de Internet».
- Organizaciones internacionales – «elaboración de normas técnicas y políticas que correspondan relativas a Internet».

El enfoque de geometría variable ha comenzado a dejarse ver en la práctica. Por ejemplo, los estados tienen un papel protagónico en la ciberseguridad y el comercio electrónico, mientras que las comunidades técnica y comercial lo tienen en la estandarización y la gestión de los nombres y números de Internet.

relacionados con la gobernanza de Internet.[16] El gran tamaño de la agenda y la limitada capacidad de políticas de los países en vías de desarrollo tanto en sus países de origen como en las misiones diplomáticas sigue siendo uno de los obstáculos más grandes para su participación total en el proceso. La necesidad de la construcción de capacidades en el campo de la gobernanza de Internet y de las políticas se reconoció como una de las prioridades para la Agenda de Túnez para la Sociedad de la Información de la CMSI

El sector comercial[18]

En los primeros días de Internet, la principal preocupación del sector comercial estaba relacionada con la protección de las marcas comerciales, ya que algunas compañías estaban enfrentándose a la ciberocupación y al uso indebido de sus marcas comerciales por individuos que eran lo suficientemente rápidos como para registrar sus nombres de dominio antes que las propias compañías. Cuando ICANN se creó, en 1998, los círculos comerciales claramente priorizaban el abordaje de la protección de las marcas comerciales. El crecimiento de Internet y del comercio electrónico ha disparado el interés del sector comercial en otras áreas, como la privacidad y la protección de datos, y otros derechos humanos en línea, la ciberseguridad, la banca electrónica, las cargas fiscales, las políticas de contenido, y el multilingüismo. Hoy en día, resulta difícil encontrar asuntos de la gobernanza de Internet que no sean de una relevancia directa para la comunidad comercial. Sin embargo, el énfasis en un asunto determinado varía según la industria.

La Cámara de Comercio Internacional

La CCI, reconocida como la asociación más importante que representa a los comercios en diferentes sectores y límites geográficos, se ha posicionado como uno de los principales representantes del sector comercial en los procesos globales de la gobernanza de Internet. La CCI tuvo una participación activa en las primeras negociaciones del GTGI y la CMSI, y continúa aportando de la misma manera en los procesos actuales del IGF.

Con el crecimiento constante de Internet, el interés de la comunidad comercial por la gobernanza de Internet se ha vuelto mayor y más diversificado. Los siguientes principales grupos de compañías han estado participando de manera activa en los procesos de la gobernanza de Internet: compañías de nombres de dominio, los PSI, las compañías de telecomunicaciones, y las compañías de contenido de Internet.

Compañías de nombres de dominio

Las compañías de nombres de dominio incluyen registros, que manejan los TLD (por ejemplo, .com y .net), y registradores que facilitan la registración de nombres de dominio para los usuarios finales. Entre los actores principales se encuentran VeriSign y Afilias. El negocio de los registros y registradores se ve influenciado directamente por las decisiones de políticas de ICANN en áreas como la introducción de nuevos TLD y la resolución de conflictos. Esto los convierte en los actores más importantes en el proceso de elaboración de políticas de ICANN. Varios registros y registradores, ya sea por medio de individuos

o asociaciones, también se han involucrado en el proceso de políticas más amplio de la gobernanza de Internet (CMSI, GTGI, IGF).

Proveedores de servicios de Internet

El rol de los PSI como intermediarios en línea clave les da una importancia particular para la gobernanza de Internet. Su principal participación se da a nivel nacional, al tratar con los gobiernos y las autoridades de aplicación de la ley. A nivel global, algunos PSI, especialmente de EE.UU. y de Europa, han tenido una participación activa en los procesos de la CMSI, el GTGI, el IGF, y ICANN; ya sea de manera individual o por medio de organizaciones nacionales, regionales, o de sectores empresariales específicos (tales como la Asociación Americana de las Tecnologías de la Información [ITAA, por sus siglas en inglés], la Asociación de Proveedores de Servicio de Internet de Europa [EuroISPA, en inglés], entre otras).

Compañías de telecomunicaciones

Las compañías de telecomunicaciones facilitan el tráfico de Internet y operan la infraestructura de Internet. Los principales actores incluyen a compañías como Verizon, AT&T, Vodafone, Deutsche Telekom, y Telefónica. Tradicionalmente, las compañías de telecomunicaciones han participado en las políticas de telecomunicaciones internacionales por medio de la UIT, y han tenido un papel cada vez más importante en las actividades de ICANN y el IGF. Su principal interés en la gobernanza de Internet es asegurar un ámbito internacional comercial amigable para fomentar un mayor desarrollo de la infraestructura de telecomunicaciones de Internet.

Además, las operadoras de telecomunicaciones plantearon la cuestión de la redistribución de las ganancias generadas gracias a la Internet. Argumentan que, siempre y cuando proporcionen acceso a Internet, deberían recibir un porcentaje mayor de los ingresos generados por Internet (que hoy en día beneficia más que nada a las compañías de contenido, debido al modelo de ingresos generados a base de publicidades).

Consulte la Sección 5 para obtener más información sobre la redistribución de las ganancias entre las compañías de Internet y de telecomunicaciones.

Las compañías de telecomunicaciones han intentado incrementar sus ingresos introduciendo nuevos servicios y solicitando a las compañías de contenido que paguen tarifas más elevadas por servicios más veloces. Varias de estas propuestas incluyen diferentes tratamientos para diferentes tipos de tráfico de Internet, lo que podría representar un incumplimiento del principio de neutralidad de la red. Esto hace que las compañías de telecomunicaciones se opongan a tal principio.

Consulte la Sección 2 para obtener más información sobre la neutralidad de la red.

En el intento de abordar el tema de la redistribución de los ingresos generados por Internet, tanto las compañías de telecomunicaciones como la industria de Internet han comenzado a ingresar una al terreno de la otra. Las compañías de telecomunicaciones

ahora proporcionan contenido de Internet y servicios de comunicación, mientras que la industria de Internet está invirtiendo en infraestructura de telecomunicaciones. Google y Facebook, por ejemplo, están invirtiendo en la instalación de cableado transatlántico y transpacífico submarino de fibra óptica.

Industria de Internet

Generalmente se conoce a la industria de la Internet como OTT. Incluye a todas las industrias cuyo modelo de negocio está basados en Internet. Se dividen en tres segmentos principales: contenido, comunicación, y servicios. La mayoría de las compañías más importantes cubren más de uno de estos segmentos. Por ejemplo, Google y Facebook proporcionan tanto contenido como servicios de comunicaciones.

Industria de CONTENIDO de la Internet

La mayor parte de la industria de Internet se basa en el contenido. El buscador de Google proporciona acceso a una gran variedad de contenido en línea. YouTube facilita acceso a material en vídeos. Facebook organiza el contenido generado por sus usuarios. Algunos de los proveedores de contenido tradicionales como Disney han evolucionado con éxito en los proveedores de contenido en línea. Las prioridades comerciales de estas compañías están muy vinculadas a los diversos asuntos de la gobernanza de Internet, tales como los DPI, la privacidad, la ciberseguridad, y la neutralidad de la red. Su presencia es cada vez más notable en los procesos globales de la gobernanza de Internet, como en la OMC, la OMPI, y el IGF.

Industria de COMUNICACIONES de la Internet

Los principales actores en los servicios de telecomunicaciones son: Skype, WhatsApp, WeChat, Snapchat, y Google Talk. La comunicación por medio de estas plataformas se encuentra cada vez más cifrada, característica que los gobiernos nacionales desafían. Por lo tanto, el principal reto para la industria de las comunicaciones de Internet es asegurar el uso de una comunicación cifrada, y la protección de los derechos a la privacidad de sus clientes.

Industria de SERVICIOS de la Internet

La industria de servicios de la Internet es también conocida como una industria de plataformas. Incluye nuevos tipos de servicios como Uber y Airbnb. Estas compañías usan Internet para proporcionar nuevos tipos de servicios, como el uso de autos privados como medio de transporte público (Uber). Su modelo de negocio está fuertemente vinculado con muchos asuntos de la gobernanza de Internet, como las cargas fiscales, la protección del consumidor, y los derechos laborales.

Sociedad civil

La sociedad civil ha promovido de manera más expresiva y activa el enfoque de múltiples partes interesadas en la gobernanza de Internet. También es la parte interesada más diversa en los procesos en este campo. Estos grupos se enfocan en los diferentes asuntos relacionados con la Internet, y varios de ellos son defensores de la protección de derechos

humanos en la Internet, que incluyen la libertad de expresión y la privacidad. La principal diferencia entre estos grupos de la sociedad civil tiene que ver con el rol de los gobiernos en la gobernanza de Internet. Tradicionalmente, los actores de la sociedad civil han visto a los gobiernos como uno entre los otros participantes iguales en los procesos de gobernanza de Internet, junto con la sociedad civil, las empresas, y la comunidad técnica. Más recientemente, ha surgido en la sociedad civil la opinión que los gobiernos deben desempeñar un papel principal en la protección de los intereses públicos, basándose en su legitimidad. En particular, esta postura se apoya en la opinión de que sólo los gobiernos pueden contrarrestar el papel muy poderoso del sector empresarial en cuestiones digitales.[19]

La gran diversidad de opiniones en los temas relacionados con la gobernanza de Internet ha complicado la coordinación de la postura de la sociedad civil en las reuniones internacionales. En el proceso de la CMSI, la representación de la sociedad civil pudo controlar esta complejidad y diversidad inherentes por medio de diferentes formas organizacionales, como la Oficina de la Sociedad Civil, el Plenario de la Sociedad Civil, y el Grupo de Contenidos y Temáticas. Debido a la naturaleza de múltiples partes interesadas del GTGI, la sociedad civil alcanzó un alto nivel de participación en este proceso. Los grupos de la sociedad civil propusieron ocho candidatos para el GTGI, que fueron todos posteriormente nombrados por el Secretario General de la ONU. Como miembros del grupo, fueron capaces de influenciar muchas conclusiones, como la decisión de crear el IGF como un espacio de múltiples partes interesadas para debatir temas sobre la gobernanza de Internet.

La sociedad civil ha continuado teniendo un rol activo en las actividades del IGF. Una de las formas de representación de la sociedad civil *sui generis* en la gobernanza de Internet es el Caucus de Gobernanza de Internet (IGC, por sus siglas en inglés). Este incluye a individuos interesados en compartir opiniones, opciones de políticas, y experticia en los asuntos sobre la gobernanza de Internet, que se discuten en un formato de listas de correo.

Las organizaciones de la sociedad civil son muy activas en casi todos los temas de la gobernanza de Internet – desde el desarrollo de infraestructura, pasando por los modelos económicos, hasta los derechos y libertades – , y se enfocan principalmente en la protección de los intereses públicos. Muchas organizaciones llenan sus vacantes con expertos y académicos con vastos conocimientos y saberes sobre las especificidades de Internet, y proporcionan valiosas contribuciones al proceso de la formación de decisiones.

Uno de los principales desafíos para estas organizaciones es la sustentabilidad de sus actividades. En los primeros tiempos del proceso de la CMSI, la mayor parte de la participación de la sociedad civil se basaba en torno a individuos comprometidos. Si bien esto contribuyó a un dinamismo desde un primer momento, también representaba un riesgo para la participación sostenible de la sociedad civil. Este tipo de participación de la sociedad civil requiere de organizaciones sostenibles. La APC ha sido uno de los primeros jugadores organizacionales involucrados en la gobernanza de Internet. Best Bytes y la Coalición Just Net también surgieron como iniciativas organizadas por la sociedad civil.

Con unos miles de millones de usuarios de Internet, la sociedad civil de Internet refleja las diversidades y diferencias de la sociedad real. Su principal desafío seguirá siendo el de representar tal diversidad de opiniones y posturas en la política digital.

Organizaciones internacionales

La UIT fue la organización internacional central en el proceso de la CMSI. Fue la sede de la Secretaría de la CMSI y proporcionaba aportes sobre políticas para los temas más importantes. La participación de la UIT en el proceso de la CMSI formaba parte de su continuo intento por definir y consolidar su nueva posición en el área de las telecomunicaciones globales de naturaleza altamente cambiante, cada vez más moldeada por la Internet. El rol de la UIT se ha visto desafiado de diferentes maneras. Por ejemplo, ha estado perdiendo su dominio sobre las políticas tradicionales debido a la liberalización del mercado global de telecomunicaciones, liderada por la OMC. La tendencia de trasladar el tráfico telefónico desde las telecomunicaciones convencionales hacia la Internet (mediante el VoIP) redujo cada vez más las huellas regulatorias de la UIT sobre el campo de las telecomunicaciones globales.

La suposición de que la UIT había sido creada a partir del proceso de la CMSI como la organización internacional de Internet *de facto* causó preocupaciones en EE.UU. y en algunos otros países desarrollados, mientras que encontró un cálido recibimiento por parte de algunos de los países en vías de desarrollo. A lo largo de la CMSI, esta suposición generó tensiones políticas subyacentes. Esto fue muy evidente en el campo de la gobernanza de Internet, en donde la tensión entre ICANN y la UIT ya existía desde el momento en que se creó ICANN en 1998. Esta tensión no fue resuelta por la CMSI pero, más tarde, desapareció bastante. Dada la creciente convergencia de distintas tecnologías de comunicaciones, es muy probable que la cuestión del rol más activo de la UIT en el área de la gobernanza de Internet se mantenga firme en la agenda política global; por ejemplo, ya está bien activa en el ámbito de la ciberseguridad y de la protección infantil en línea.

Otro de los problemas estaba relacionado con el afianzamiento de la agenda multidisciplinaria de la CMSI dentro del conjunto de agencias especializadas de la ONU. Los aspectos no técnicos de las comunicaciones y de la tecnología de la Internet, como los sociales, económicos, y culturales, son parte de las misiones de otras organizaciones de la ONU. La más importante en este contexto es la UNESCO, que aborda temas relacionados con el multilingüismo, la diversidad cultural, la sociedad del conocimiento, y el intercambio de información. La OMPI también muestra un papel activo en los debates sobre la gobernanza de Internet, especialmente en temas relacionados con la protección de los IPR en el espacio digital.

El equilibrio entre la UIT y otras organizaciones de la ONU fue controlado con suma precaución. Los procesos de seguimiento de la CMSI también reflejan tal equilibrio, con el papel coordinador de la UIT y la participación de la UNESCO, el PNUD, y la UNCTAD. Estas agencias de la ONU son, por ejemplo, las principales encargadas de organizar el Foro anual de la CMSI, que, en los últimos años, ha incluido cada vez más debates sobre temas concernientes a la gobernanza de Internet.

La comunidad técnica

La comunidad técnica está integrada por instituciones e individuos que de alguna manera han participado en el desarrollo de la Internet y/o administran sus recursos técnicos. Esta comunidad también ha creado el espíritu inicial de la Internet, que se basa en los principios de intercambio de recursos, acceso abierto, y oposición a la participación gubernamental en la regulación de Internet. Desde el comienzo, sus miembros han protegido el

concepto inicial de la Internet, alejado de la comercialización y la influencia gubernamental extensiva.

Terminología: comunidad técnica

Se pueden usar otros términos, indistintamente, para referirse a la «comunidad técnica»: comunidad de Internet, desarrolladores de Internet, fundadores de la Internet, padres de la Internet, y tecnólogos. El término «comunidad técnica» se usa en las declaraciones de la CMSI y en otros documentos de políticas.

La comunidad técnica cumple con todos los criterios de la definición propuesta por Peter Haas[20] para la comunidad epistémica: «grupo profesional que cree en las mismas relaciones de causa y efecto, realiza pruebas de veracidad para aceptarlas, y comparte valores en común. Sus miembros comparten un entendimiento en común acerca de un problema y sus soluciones».relationships, truth tests to accept them, and shares common values; its members share a common understanding of a problem and its solutions'.

La comunidad técnica en sus principios estaba coordinada por algunas reglas (principalmente tácitas) y por un procedimiento formal principal: las RFC. Estas últimas describen todos los estándares principales y básicos de la Internet. A pesar de que no contaba con una regulación estricta ni una estructura formal, la comunidad de Internet en sus primeras etapas estaba regida por costumbres bien arraigadas y por la presión generada entre pares. La mayoría de los participantes en este proceso compartían valores, sistemas de apreciación, y actitudes similares.

La gestión temprana de la Internet por parte de la comunidad técnica se vio desafiada a mediados de la década de 1990, luego de que la Internet se volvió parte de la vida social y económica del mundo entero. Su crecimiento introdujo un nuevo grupo de partes interesadas, como el sector comercial, que trajo consigo diferentes culturas profesionales y un entendimiento de la Internet y su gobernanza propio. Esto causó una creciente tensión en el ámbito de Internet. Por ejemplo, en la década de 1990, la comunidad de Internet y la compañía Network Solutions[21] se vieron enfrentadas en la denominada Guerra del DNS, un conflicto a causa del control del servidor raíz y el sistema de nombres de dominio.

La Internet Society es uno de los representantes más importantes de la comunidad técnica. La IETF forma parte de ella, apoya la causa por una Internet abierta, y desempeña un papel activo en el desarrollo de capacidades.

La comunidad técnica ha sido un actor importante en los procesos de creación y de administración de ICANN. Uno de los padres de la Internet, Vint Cerf, fue el director de la Junta de ICANN desde el 2000 hasta 2007. Algunos miembros de la comunidad técnica poseen puestos de gran importancia en varios organismos de toma de decisiones de ICANN.

Hoy en día, con más de tres mil millones de usuarios, la Internet ha crecido demasiado para el marco inicial de políticas de ICANN, que se enfoca en la comunidad técnica como su componente principal. Desde esta perspectiva, debido a que la línea que divide a los ciudadanos y a los usuarios de Internet no es muy clara, se requiere mayor participación por parte de los gobiernos y de otras estructuras que representen a los ciudadanos en lugar de aquellas que representan a los usuarios de Internet pura y exclusivamente (forma en la

que se ha descripto a la comunidad técnica). Aquellos que favorecen la participación del gobierno en la gobernanza de Internet utilizan este enfoque de representación de ciudadanos en vez del de los usuarios y las comunidades de Internet.

La justificación que utiliza regularmente la comunidad técnica con respecto a su posición privilegiada en ciertos procesos en la gobernanza de Internet es su experticia técnica. Asevera que ICANN es principalmente una organización técnica, y que, por lo tanto, los técnicos en contacto con los conocimientos específicos deberían administrarla. Debido a la creciente dificultad de mantener a ICANN como una organización pura y exclusivamente técnica, esta justificación se ha enfrentado a frecuentes discusiones. Es altamente probable que los miembros de la comunidad técnica se integren, poco a poco, a otros grupos de partes interesadas: principalmente la sociedad civil, el sector comercial, y el sector académico, así como también a los gobiernos.

ICANN

La ICANN fue creada en 1998 como una corporación sin fines de lucro con sede en EE.UU. El gobierno de los Estados Unidos le concedió la tarea de llevar a cabo las funciones de la IANA (es decir, la administración general de la infraestructura básica de la Internet, que consiste en direcciones IP, nombres de dominio, y servidores raíz).

El creciente interés por el rol de ICANN se desarrolló en paralelo al rápido crecimiento de la Internet a principios del nuevo milenio. Así, ICANN se llevó la atención de los círculos de políticas globales durante el proceso de la CMSI (2003-2005).

La misión actual de ICANN, según se refleja en su reglamento revisado de 2016, es la de asegurar la operación estable y segura de los sistemas de identificadores únicos de la Internet. Con este propósito, la organización coordina la distribución y la asignación de los nombres en la zona raíz del DNS, así como el desarrollo y la implementación de políticas concernientes a los gTLD; también facilita la coordinación del sistema de servidor de nombres raíz del DNS; y coordina la distribución y asignación generales de los números IP y los números de sistema autónomos.

Si bien ICANN es uno de los principales actores en el campo de la gobernanza de Internet, no gobierna todos sus aspectos. En ocasiones se ha dicho, aunque de manera errónea, que es el gobierno de la Internet. La ICANN gestiona los recursos técnicos de Internet pero no posee autoridad directa sobre otras áreas de la gobernanza de Internet, como la ciberseguridad, la política de contenidos, la protección del derecho de autor, la protección de la privacidad, la conservación de la diversidad cultural, y la disminución del dividendo digital.

La ICANN es una institución de múltiples partes interesadas compuesta por varios actores con diferentes capacidades y roles. Estos se pueden categorizar en tres grupos:

- Las comunidades técnica y comercial, cuyo rol dentro de ICANN es el de desarrollar recomendaciones para la Junta de ICANN sobre políticas que cubren las áreas relacionadas con la misión de la organización (por ejemplo, los gTLD, la seguridad y estabilidad del DNS, etc.).

- Los gobiernos nacionales, cuyo creciente interés por tener un rol más importante en ICANN comenzó en el proceso de la CMSI. En el marco del proceso de desarrollo de políticas de ICANN, los gobiernos cumplen un papel asesor: aconsejan a la Junta de

ICANN, particularmente sobre los asuntos que podrían afectar a los temas de políticas públicas.

- Los usuarios de Internet (la comunidad en general), cuya contribución en el proceso de desarrollo de políticas es también de carácter consultivo.

Involucrar a los usuarios de Internet

La ICANN ha experimentado con varios enfoques para involucrar a los usuarios de la Internet. En sus primeros días, el primer intento fue el de involucrar a los usuarios de Internet mediante elecciones directas para elegir los representantes de los organismos de gobierno de la ICANN. Este intento tenía el propósito de asegurar la legitimidad de ICANN. Como resultado de una escasa participación y de un uso indebido del proceso, la votación directa no tuvo éxito: no proporcionaba una representación real de los usuarios de Internet. Más tarde, ICANN comenzó a darles participación a los usuarios de Internet por medio de una estructura de gobernanza «at-large» (Comité Asesor At-Large [ALAC, por sus siglas en inglés]), y también por medio de consultas populares, y de la «colaboración abierta distribuida», más conocida como *outsourcing*.[22] Estos experimentos organizacionales son esenciales para asegurar la legitimidad de ICANN.

El proceso de toma de decisiones de ICANN se vio influenciado por los primeros procesos de la gobernanza de Internet, basados en enfoques ascendentes, transparentes, abiertos, e inclusivos. La principal diferencia entre la comunidad técnica inicial (de la década de 1980) y el contexto actual del proceso de toma de decisiones de ICANN es el nivel de «capital social». En el pasado, la comunidad técnica contaba con niveles elevados de confianza mutua y solidaridad, lo que facilitaba la toma de decisiones y la resolución de conflictos mucho más que hoy en día. El crecimiento de la Internet se extendió a miles de millones de nuevos usuarios y nuevas partes interesadas, lo que comprendía un rango mucho más amplio que la comunidad técnica inicial. Como resultado, este rápido crecimiento de la Internet redujo el capital social que existía en sus primeros días. Así, las propuestas frecuentes de la comunidad técnica para mantener el proceso inicial, informal, y de toma de decisiones en Internet no han sido realistas. Sin capital social, la única manera de asegurar un proceso de toma de decisiones completamente funcional es formalizarlo y desarrollar diferentes mecanismos de pesos y contrapesos.

Ya se introdujeron algunas correcciones a los procedimientos de la toma de decisiones para reflejar esta realidad cambiante. Por ejemplo, la reforma de ICANN de 2002 incluyó el fortalecimiento del GAC y el abandono del sistema de votación directa para los usuarios de Internet. Actualmente, se están implementando más cambios con el objetivo de incrementar la rendición de cuentas de ICANN en lo que respecta a la comunidad global de Internet.

Los asuntos

La gestión técnica vs la gestión de políticas

La dicotomía entre la gestión técnica y la gestión de políticas ha creado una continua tensión en las actividades de ICANN. Esta se ha representado a sí misma como el organismo de coordinación técnica para la Internet, que se ocupa específicamente de los asuntos

técnicos y se mantiene apartado de los aspectos de las políticas públicas de Internet. Los funcionarios de ICANN consideraron esta naturaleza meramente técnica como el principal argumento conceptual para defender el estatus excepcional de la institución y su estructura organizacional. La primera presidente de ICANN, Esther Dyson, enfatizó que: «ICANN no "aspira a abordar" asuntos relacionados con la gobernanza de Internet; en realidad, gobierna las instalaciones, no la gente. Posee la función acotada de administrar ciertos aspectos (en su mayoría técnicos) de la infraestructura de Internet en general y del Sistema de Nombres de Dominio en particular».[23]

Los críticos de esta afirmación generalmente hacen referencia al hecho de que no existe solución técnicamente neutral alguna. Tarde o temprano, cada solución o decisión técnica promueve ciertos intereses, empodera a ciertos grupos, y afecta la vida social, política, y económica. El abordaje de temas como el TLD .xxx y los nuevos gTLD incorporados en 2014 ilustra cada vez más el hecho de que ICANN debe tratar con temas técnicos de los aspectos de políticas públicas.

Transición de la administración de la IANA y rendición de cuentas de ICANN

Hasta el 1 de octubre de 2016, la ICANN llevaba a cabo las funciones de la IANA sobre la base de un contrato con el gobierno de los Estados Unidos (el Departamento de Comercio, mediante la NTIA). Según este contrato, el gobierno de EE.UU. poseía la máxima autoridad sobre cualquier cambio significativo dentro del DNS (por ejemplo, cuando la ICANN decidió aprobar nuevos gTLD determinados; cada una de estas decisiones además necesitaba la validación formal del gobierno de los EE. UU.).

En marzo de 2014, el gobierno de EE.UU. anunció su intención de transferir su rol administrativo sobre las funciones de la IANA a la comunidad global de múltiples partes interesadas.[24] Se le solicitó a ICANN lanzar un proceso para el desarrollo de una propuesta de transición. Al mismo tiempo, se llevaron a cabo trabajos sobre la elaboración de un conjunto de recomendaciones para mejorar los mecanismos de rendición de cuentas de ICANN. Entre 2014 y 2016, la comunidad de ICANN realizó un trabajo exhaustivo sobre la elaboración de las propuestas de transición y rendición de cuentas, que en marzo de 2016 fueron aprobadas por la Junta de ICANN, y en junio de 2016, aceptadas por el gobierno de EE.UU., ya que cumplían con todos sus requisitos.

De acuerdo con la propuesta de transición de la administración de la IANA, la ICANN creó los PTI, como la subsidiaria que se convirtió en el operador de las funciones de asignación de nombres de la IANA, sobre la base de un contrato con ICANN. Esto significa que las funciones de la IANA relacionadas con los nombres de dominio continúan rigiéndose según el marco de ICANN, pero con una división más clara entre las funciones técnicas y las funciones de elaboración de políticas de ICANN. El reglamento revisado de ICANN, en vigencia desde el 1 de octubre de 2016, también resalta la condición bajo la que un proceso de revisión podría causar la separación de los operadores de las funciones de la IANA de ICANN. Algunos cambios significativos en la zona raíz del DNS (previamente sujetos a la aprobación formal por parte del gobierno de EE.UU.) están ahora sujetos a la validación de la Junta de Directores de la ICANN.

El desempeño de las funciones de la IANA relacionadas con los números IP y los parámetros de protocolos también ha sido trasladado a los PTI. Se celebraron acuerdos para el desempeño de estas funciones entre ICANN y la comunidad de los recursos de numeración (principalmente los RIR responsables de la distribución regional y la gestión de las direcciones IP), y la comunidad de parámetros de protocolos (representada por la IETF y la IAB), y fueron seguidos por acuerdos de subcontratación entre ICANN y los PTI.

Con respecto a la rendición de cuentas de ICANN ante la comunidad de Internet en general, y ante la ausencia del rol administrativo del gobierno estadounidense, se han implementado nuevos mecanismos dentro de la organización. El más importante es la creación de una nueva entidad legal – la comunidad empoderada – que funciona como una asociación no incorporada que posee la habilidad de aplicar el cumplimiento de un conjunto de poderes comunitarios, como el poder de destituir a miembros de la Junta de ICANN, rechazar presupuestos de ICANN, o rechazar cambios para los reglamentos de ICANN. Esta entidad actúa bajo la instrucción de las decisiones de sus participantes: la mayoría de los comités asesores de ICANN y las organizaciones de apoyo que representan a los usuarios de la Internet, los gobiernos, el sector privado, y la comunidad técnica.[25]

NOTAS FINALES

[1] A menudo se toma al modelo brasileño de gestión de nombres de dominio del país como un ejemplo exitoso de un enfoque de múltiples partes interesadas. El organismo nacional responsable de los dominios brasileños – el CGI – se encuentra abierto a todos los usuarios, incluidos las autoridades de gobierno, el sector comercial, y la sociedad civil. Poco a poco, Brasil ha extendido este modelo a otras áreas de la gobernanza de Internet, especialmente en el proceso de preparación para el IGF 2007 y 2014, que se llevaron a cabo en Río de Janeiro, y João Pessoa, respectivamente. Brasil ha mantenido un rol activo en la gobernanza de Internet, en especial en NetMundial (http://netmundial.br), un proceso iniciado en octubre de 2013 por la presidente brasileña Dilma Rousseff y el presidente de ICANN Fadi Chehadé, y en el proceso de seguimiento, la Iniciativa de NetMundial (https://www.netmundial.org/).

[2] Para obtener una lista actualizada de las iniciativas nacionales del IGF, consulte el Foro de Gobernanza de Internet (sin fecha) Iniciativas Nacionales del IGF. Disponible en http://www.intgovforum.org/multilingual/content/national-igf-initiatives [accedido el 6 de noviembre de 2016]. El sitio web del IGF incluye una lista de las iniciativas regionales reconocidas del IGF: Foro de Gobernanza de Internet (sin fecha) Iniciativas Regionales del IGF. Disponible en http://www.intgovforum.org/multilingual/content/regional-igf-initiatives [accedido el 6 de noviembre de 2016].

[3] Géraud A (1954) The rise and fall of the Anglo-French Entente. *Foreign Affairs*. Disponible en http://www.foreignaffairs.com/articles/71095/andre-geraud-pertinax/rise-and-fall-of-the-anglo-french-entente [accedido el 29 de octubre de 2016].

[4] Lesage C (1915) *La rivalite franco-britannique. Les cables sous-marins allemands* París. p. 257–258; citado en: Headrick D (1991) *The Invisible Weapon: Telecommunications and International Politics 1851–1945*. Oxford: Oxford University Press. p. 110.

[5] Mueller M (1999) ICANN and Internet governance: Sorting through the debris of 'self-regulation'. *info (The Journal of Policy, Regulation and Strategy for Telecommunications Information and Media)* 1(6), pp. 497–520. Disponible en http://www.icannwatch.org/archive/mueller_icann_and_Internet_governance.pdf [accedido el 14 de marzo de 2016].

[6] Secretario de Estado de Estados Unidos en crítica a la UIT por su iniciativa: «sin la autorización de los gobiernos miembros para llevar a cabo un encuentro global que implicara un gasto de recursos no autorizado y por celebrar acuerdos internacionales». Citado en Drake W. (2004) Reframing Internet Governance Discourse: Fifteen Baseline Propositions, p. 9. Disponible en https://www.un-ngls.org/orf/drake.pdf [accedido el 29 de octubre de 2016].

[7] Internet World Stats (2015) Internet Usage in the European Union. Disponible en http://www.Internetworldstats.com/stats9.htm [accedido el 14 de noviembre de 2016].

[8] Comisión Europea (2013) Antitrust: Commission seeks feedback on commitments offered by Google to address competition concerns. Comisión Europea – IP/13/371. Disponible en http://europa.eu/rapid/press-release_IP-13-371_en.htm [accedido el 29 de octubre de 2016].

[9] Grupo Alibaba (sin fecha) Plataforma Electrónica de Comercio Mundial. Disponible en http://www.alizila.com/wp-content/uploads/2016/09/eWTP.pdf [accedido el 12 de noviembre de 2016].

[10] Ministro de Relaciones Exteriores de la República Popular de China (2015) Comentarios por S.E. Xi Jinping, Presidente de la República Popular de China en la ceremonia inaugural de la Segunda Conferencia Mundial de Internet. Disponible en http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml [accedido el 12 de noviembre de 2016].

[11] Rousseff D (2013) Declaración por S. E. Dilma Rousseff, presidente de la República Federativa de Brasil, en la apertura del debate general del 68° periodo de sesiones de la Asamblea General de la ONU. Disponible en https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf [accedido el 29 de octubre de 2016].

[12] NETmundial (2014) Declaración de Múltiples Partes Interesadas NETmundial. Disponible en http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf [accedido el 29 de octubre de 2016].

[13] Goldstein D (2016) Indian Minister of Electronics and Information Technology Reaffirms Support of the Multistakeholder Model at ICANN's 57th Public Meeting. *Domain Pulse*, 6 de noviembre. Disponible en http://www.domainpulse.com/2016/11/06/india-reaffirms-support-multistakeholder-model-icann57/ [accedido el 6 de noviembre de 2016].

[14] Asamblea General de las Naciones Unidas (1999) Resolución A/53/70. Los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. Disponible en http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70 [accedido el 8 de noviembre de 2016].

[15] Radu R (2013) Negotiating meanings for security in the cyberspace. *Info* 15(6), pp. 32-41. Disponible en https://www.researchgate.net/publication/255697155_Negotiating_meanings_for_security_in_the_cyberspace [accedido el 14 de marzo de 2016].

[16] La conveniencia de compra por «ventanilla única» fue uno de los argumentos para que la UIT se estableciera como el jugador central de la gobernanza de Internet.

[17] CMSI (2003) Declaración de Principios. Disponible en http://www.itu.int/wsis/docs/geneva/official/dop.html [accedido el 12 de noviembre de 2016].

[18] Ayesha Hassan contribuyó con valiosos comentarios.

[19] Esta opinión ha sido apoyada, en particular, por la Just Net Coalition, y se refleja en varias declaraciones y declaraciones emitidas por la organización. Para obtener más información, consulte Just Net Coalition (sin fecha) Declaraciones. Disponible en http://justnetcoalition.org/statements [accedido el 10 de noviembre de 2016].

[20] Haas P (1990) *Saving the Mediterranean: The Politics of International Environmental Cooperation*. Nueva York: Columbia University Press, p.55

[21] La compañía tecnológica Network Solutions www.networksolutions.com fue fundada en 1979. El negocio del registro de nombres de dominio era la división más importante de la compañía; la compañía diversificó su cartera para incluir servicios web para las pequeñas empresas.

[22] Radu R *et al*. (2015) Crowdsourcing ideas as an emerging form of multistakeholder participation in Internet governance. *Policy & Internet* 7(3), pp. 362–382

[23] Dyson E (1999) *Esther Dyson's response to Ralph Nader's Questions*. Disponible en http://www.icann.org/en/correspondence/dyson-response-to-nader-15jun99.htm [accedido el 14 de marzo de 2016].

[24] NTIA (2014) La NTIA anuncia la intensión de trasferir funciones clave de nombre de dominio de Internet. Disponible en https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-Internet-domain-name-functions [accedido el 29 de octubre de 2016].

[25] Para obtener más detalles sobre la transición de la administración de la IANA y los procesos de rendición de cuentas de ICANN, consulte el observatorio de *GIP Digital Watch* (sin fecha) IANA Transition and ICANN Accountability. Disponible en http://digitalwatch.giplatform.org/processes/iana [accedido el 29 de octubre de 2016].

DiploFoundation es una organización sin fines de lucro dedicada a lograr que la diplomacia y la gobernanza internacional sean más inclusivas y eficaces. En particular, Diplo trabaja para

- Aumentar el poder de los estados pequeños y en desarrollo para participar de manera significativa en los asuntos internacionales.
- Aumentar la rendición de cuentas y la inclusión internacionales.
- Aumentar la legitimidad de la elaboración de políticas internacionales.
- Mejorar la gobernanza mundial y el desarrollo de políticas internacionales.

Las principales actividades de Diplo incluyen:

El desarrollo de capacidades: El apoyo del desarrollo de capacidades de Diplo empieza con los individuos, que por medio de sus actividades, nuestro impacto alcanza a sistemas más grandes de los que forman parte ellos y sus organizaciones. Nuestro enfoque incluye la capacitación en línea, la investigación de políticas, la inmersión política, y el desarrollo de comunidades de práctica, combinadas de varias maneras, según cada contexto político. Entre los temas del desarrollo de las capacidades se encuentra la gobernanza de Internet, la diplomacia electrónica, la diplomacia pública, la diplomacia humanitaria, y la diplomacia mundial en temas de salud.

Eventos: Para enfrentar las cuestiones apremiantes en la gobernanza de Internet, nuestros eventos reúnen a personas con diferentes puntos de vista, como diplomáticos, profesionales de negocios, y miembros de la sociedad civil. Nos esforzamos para que nuestros eventos sean más accesibles mediante herramientas electrónicas que habilitan la participación remota. Por lo general, nuestros eventos se convierten en actividades de capacitación, publicaciones, o interacción en línea.

Cursos: Ofrecemos cursos académicos de posgrado y talleres de capacitación en una variedad de temas relacionados con la diplomacia que están dirigidos a diplomáticos, funcionarios públicos, personal de organizaciones internacionales y ONG, y estudiantes de relaciones internacionales. Al combinar una metodología de aprendizaje desarrollada con nuestra única plataforma de aprendizaje en línea, nuestros cursos son flexibles, personalizados, interactivos, y de formación comunitaria. Los cursos son en línea, presenciales, y en un formato combinado.

Investigación: Avanzamos en los métodos de investigación de políticas tradicionales mediante técnicas basadas en Internet, como la colaboración colectiva, el análisis de tendencias, y la investigación conjunta. Los temas de investigación son: la diplomacia, la gobernanza de Internet, el aprendizaje en línea, entre otros.

Publicaciones: Nuestras publicaciones varían desde la evaluación de los desarrollos contemporáneos en la diplomacia hasta los nuevos análisis de sus aspectos tradicionales. Muchas de nuestras publicaciones están disponibles en línea así como también en formato papel, y algunas están traducidas a varios idiomas.

Diplo fue fundada en 2002 por los gobiernos de Malta y Suiza, y cuenta con oficinas en Msida, Malta; Ginebra, Suiza; y Belgrado, Serbia. Diplo tiene estatus consultivo ante el ECOSOC de las Naciones Unidas desde 2006.

Para obtener más información sobre Diplo, visite https://www.diplomacy.edu

Geneva Internet Platform

El Departamento Federal de Asuntos Exteriores (DFAE) de suiza y la Oficina Federal de Comunicaciones (OFCOM) iniciaron la **Geneva Internet Platform** (GIP), que cumple su misión como observatorio, centro de construcción de capacidades (en línea e *in situ*), y centro para el debate. La GIP es una iniciativa respaldada por las autoridades de Suiza y operada por DiploFoundation.

Sus actividades se implementan sobre la base de tres pilares:
- Una plataforma física en Ginebra
- Una plataforma en línea y observatorio
- Un laboratorio de innovación

Se enfoca especialmente en asistir a países pequeños y en desarrollo para que participen de manera significativa en los procesos de la gobernanza de Internet. El apoyo se ajusta a las necesidades de estos actores; e incluye la capacitación, la concientización, el asesoramiento, y las reuniones informativas (briefings).

Para obtener más información sobre las actividades de la GIP, visite
http://www.giplatform.org

DigitalWatch

La *GIP Digital Watch* tiene la finalidad de brindar a los profesionales de la gobernanza de Internet y políticas digitales una herramienta que les permita mantenerse actualizados con la información sobre los temas de políticas de Internet, los participantes, y los desarrollos en curso. El GIP Digital Watch se basa en materiales, experticia de gestión de conocimientos y redes desarrolladas por DiploFoundation durante los últimos 20 años.

Son tres los pilares que forman parte de la iniciativa *GIP Digital Watch*:

La *Observatorio de GIP Digital Watch* proporciona un centro único neutral para los desarrollos en vivo, las revisiones y los textos expositivos, eventos, los recursos, y otros contenidos relacionados con la gobernanza de Internet y las políticas digitales.

El *Boletín de Geneva Digital Watch*, es un boletín informativo mensual que incluye un resumen sobre los desarrollos, las entrevistas con expertos reconocidos, y los artículos sobre varias áreas de las políticas digitales.

Las reuniones informativas mensuales de la GIP sobre la gobernanza de Internet en Ginebra y en línea se llevan a cabo el último martes de cada mes. A partir de 2016, se están instalando núcleos locales en todo el mundo para incentivar los debates sostenibles en las comunidades locales, y compartir las perspectivas regionales durante las reuniones informativas mensuales.

Para obtener más información sobre la GIP Digital Watch, visite
http://digitalwatch.giplatform.org/

Glosario

3G	redes móviles de tercera generación
4G	redes móviles de cuarta generación
5G	redes móviles de quinta generación
ACTA	Acuerdo Comercial Anti-falsificación
ADR	Resolución Alternativa de Conflictos
AFRINIC	Registro Regional de Internet para Africa
AFTLD	Asociación Africana de Registros de Primer Nivel
AGONU	Asamblea General de las Naciones Unidas
ALAC	Comité Asesor At-Large (ICANN)
APC	Asociación para el Progreso de las Comunicaciones
APEC	Cooperación Económica de Asia Pacífico
APNIC	Registro Regional de Internet para Asia Pacífico
APTLD	Asociación de Asia Pacífico de Registros de Primer Nivel
ARF	Foro Regional de la Asociación de Naciones del Sudeste Asiático
ARPANet	Agencia de Proyectos de Investigación Avanzada para la Defensa (EE.UU.)
ARIN	Registro Regional de Internet para Norte América
ASEAN	Asociación de Naciones del Sudeste Asiático
AXIS	Sistema Africano de Intercambio de Internet (AU)
BEREC	Organismo de Reguladores Europeos de Comunicaciones Electrónicas
BGPSec	Protocolo de Seguridad Border Gateway
BPI	Banco de Pagos Internacionales
BRICS	Brasil, Rusia, India, China, y Sudáfrica
BTA	Convenio de Telecomunicaciones Básicas
CA	Autoridades de Certificación
CBM	medidas de construcción de confianza
CCD COE	Centro de Excelencia OTAN de Ciberdefensa Cooperativa
CCI	Cámara de Comercio Internacional
ccNSO	Organización de Apoyo para Nombres de Dominio con Código de País (ICANN)
CCTD	Comisión de Ciencia y Tecnología para el Desarrollo de la ONU
ccTLD	código de país de nivel superior
CdE	Consejo de Europa
CDH de la ONU	Consejo de Derechos Humanos de la ONU
CDN	Convención sobre los Derechos del Niño (de la ONU)
CDN	Red de Entrega de Contenidos
CDPD	Convención sobre los Derechos de las Personas con Discapacidad de la ONU

CEDAW	Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer de la ONU
CEFACT	Centro para la Facilitación del Comercio y el Comercio Electrónico (ONU)
CEN	Comité Europeo de Normalización
CENTR	Consejo Europeo de Registros Nacionales de Dominios de Nivel Superior
CERN	Organización Europea para la Investigación Nuclear
CERT	Equipo de Respuesta ante Emergencias Informáticas
CGI.br	Comité gestor de internet en Brasil
CI	infraestructura crítica
CIA	confidencialidad, integridad, y disponibilidad
CICTE	Comité Interamericano contra el Terrorismo
CIDR	Enrutamiento entre Dominios sin Clases
CIGF	Foro de Gobernanza de Internet de la Commonwealth
CII	Infraestructura Crítica de Información
CIIP	protección de la infraestructura crítica de la información
CIR	recursos críticos de Internet
CITEL	Comisión Interamericana de Telecomunicaciones
CMSI	Cumbre Mundial sobre la Sociedad de la Información
CMTI	Conferencia Mundial de Telecomunicaciones Internacionales
CND	Red de Entrega de Contenidos
CNUDMI	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
COMESA	Mercado Común de África Oriental y Austral
COP	Protección de la Infancia en Línea (Iniciativa UIT)
CORE	Consejo de Registradores
CSIRT	Equipo de Respuesta frente a Incidentes de Seguridad Informática
CSS	Hojas de estilo en cascada
DDoS	ataque de denegación de servicio distribuido
DMCA	Ley de Derechos de Autor de la Era Digital (EE.UU.)
DNS	Sistema de Nombres de Dominio
DNSSEC	Extensiones de Seguridad para el Sistema de Nombres de Dominio
DoS	Denegación de servicio
DSL	Líneas de Suscripción Digital
DUDH	Declaración Universal de Derechos Humanos
DWDM	multiplexado compacto por división en longitudes de onda
ebXML	electronic business XML
ECOSOC	Consejo Económico y Social (de la ONU)
ECTS	Sistema europeo de transferencia y acumulación de créditos
EDI	Intercambio electrónico de datos
eIDAS	Reglamento de identificación electrónica y servicios de confianza digitales para las transacciones electrónicas en el mercado interior

ENISA	Agencia Europea de Seguridad de las Redes y de la Información
EPC	Códigos Electrónicos de Productos
EPCIP	Programa Europeo de Protección de Infraestructuras Vitales
ETNO	Asociación Europea de Operadores de Redes de Telecomunicaciones
ETSI	Instituto Europeo de Estándares de Telecomunicaciones
EuroDIG	Diálogo Europeo sobre la Gobernanza de Internet
EuroISPA	Asociación de proveedores de servicio de internet de Europa
Europol	Oficina Europea de Policía
FATF	Fuerza de Trabajo de Acción Financiera
FBI	Oficina Federal de Investigaciones (EE.UU.)
FCC	Comisión Federal de Comunicaciones (EE.UU.)
FEM	Foro Económico Mundial
FIRST	Foro Internacional de Equipos de Respuesta a Incidentes y Seguridad
FMI	Fondo Monetario Internacional
GAC	Comité Asesor Gubernamental (ICANN)
GATS	Acuerdo General sobre el Comercio de Servicios
GATT	Acuerdo General sobre Aranceles Aduaneros y Comercio
GCA	Agenda sobre ciberseguridad global
GCCS	Conferencia Global sobre el Ciberespacio
GFCE	Foro Global de Experticia Cibernética
GGE	Grupo de Expertos Gubernamentales sobre los Avances en el campo de la Información y las Telecomunicaciones en el Contexto de Seguridad Internacional de la ONU
GICGM	panel de Alto Nivel sobre Corporación Global y Mecanismo de Gobernanza de Internet
GIP	Geneva Internet Platform
GSM	Sistema Global para las Comunicaciones Móviles
GSMA	Groupe Speciale Mobile Association
GTGI	Grupo de Trabajo sobre Gobernanza de Internet
gTLD	dominio genérico de nivel superior
HD	Alta definición
HTCIA	Asociación sobre Investigación de Delitos de Alta Tecnología
HTML	HyperText markup language
HTTP	Protocolo de Transferencia de Hipertexto
IA	Inteligencia Artificial
IaaS	infraestructura como servicio
IAB	Junta de Arquitectura de Internet
IANA	Autoridad de Asignación de Números Internet
IBP	Proveedor de Internet de ancho de banda
ICANN	Corporación para la Asignación de Nombres y Números en Internet
ICMEC	Centro Internacional para Niños Desaparecidos y Explotados
IDC	Corporación Internacional de Datos
IDN	nombre de dominio internacionalizado

IEEE	Instituto de Ingeniería Eléctrica y Electrónica
IETF	Fuerza de Tareas de Ingeniería de Internet
IGC	Caucus de Gobernanza de Internet
IGF	Foro de Gobernanza de Internet
IMC	Índice Mundial de Ciberseguridad
IMPACT	Alianza Internacional Multilateral contra las Ciberamenazas
INHOPE	Asociación Internacional de Líneas Directas de Denuncia de Internet
INSAFE	Red de Centros para una Internet más Segura
INTERPOL	Organización Internacional de Policía Criminal
IoT	Internet de las Cosas
IP	protocolo de Internet
IPR	Derechos de Propiedad Intelectual
IPSec	seguridad del Protocolo de Internet
IPTV	televisión por protocolo de Internet
IPv4	Protocolo de Internet versión 4
IPv6	Protocolo de Internet versión 6
IRP	Proceso de Revisión Independiente
ISO	Organización Internacional de Normalización
ITAA	Asociación Americana de las Tecnologías de la Información
IVA	Impuesto al valor agregado
IXP	Punto de intercambio de tráfico de Internet
LACNIC	Registro Regional de Internet para América Latina y el Caribe
LACTLD	Organización de ccTLD de América Latina y el Caribe
LAN	Redes de Área Local
LED	diodos emisores de luz
LGBT	Comunidad de Lesbianas, Gays, Bisexuales, y personas Transgénero
LIR	Registro de Internet local
LPWAN	redes amplias de bajo consumo
LTE	Evolución a largo plazo
M3AAWG	Grupo de Trabajo Anti-Abuso vía Mensajería, Malware y Móviles
MDG	objetivos de desarrollo del milenio
MIS-NET	Comité de expertos sobre intermediarios de Internet (CdE)
MLAT	Tratados de Asistencia Legal Mutual
MoU	memorándum de entendimiento
NAT	Traducción de Direcciones de Red
NIR	registros de Internet nacionales
NRI	Índice de Disponibilidad de Red (FEM)
NSA	Agencia de Seguridad Nacional de EE. UU
NSI	Network Solutions Inc.
NTIA	Administración Nacional de Telecomunicaciones e Información (EE.UU.)
OASIS	Organización para el Avance de Estándares de Información Estructurada
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OCS	Organización de Cooperación de Shanghái

ODR	Resolución de Litigios en línea
ODS	objetivos de desarrollo sostenible
OEA	Organización de las Estados Americanos
OIT	Organización Internacional del Trabajo
OMC	Organización Mundial del Comercio
OMPI	Organización Mundial de la Propiedad Intelectual
ONU	Organización de las Naciones Unidas
OSCE	Organización para la Seguridad y la Cooperación en Europa
OTAN	Organización del Tratado del Atlántico Norte
OTT	servicios over-the-top
P2P	entre pares
PaaS	plataforma como servicio
PIPA	ley PROTECT IP
PKI	infraestructura de clave pública
PLC	comunicaciones mediante línea de potencia
PMA	Países Menos Adelantados
PPP	asociaciones público-privadas
PRISM	El proyecto de metodología para el registro de información personal
PSI	Proveedor de Servicios de Internet
PTI	Identificadores Técnicos Públicos (ICANN)
PYME	Pequeñas y medianas empresas
QoS	calidad de servicio
REMJA	Ministros de Justicia y otros Ministros, Procuradores, o Fiscales Generales de las Américas
RFC	request for comments
RFID	Identificación por radiofrecuencia
RIPE	NCC Centro de Coordinación de Redes IP Europeas
RIR	Registro Regional de Internet
RSC	Comité del Espectro Radioeléctrico (UE)
RSPG	Grupo de Política del Espectro Radioeléctrico (UE)
RTI	Reglamento de Telecomunicaciones Internacionales
SaaS	software como servicio
SCADA	supervisión, control, y adquisición de datos
SGML	Lenguaje de Marcado Generalizado Estándar
SNA	arquitectura de red de sistemas
SOPA	Acta de Cese de Piratería en Línea
SOX	Ley Sarbanes-Oxley
SSL	capa de puertos seguros
TACD	Diálogo Transatlántico de Consumidores
TASIM	Superautopista Transeuroasiática de la Información
TCP/IP	Protocolo de Control de Transmisión/Protocolo de Internet
TEDH	Tribunal Europeo de Derechos Humanos
TIC	tecnologías de la información y comunicación
TJUE	Tribunal de Justicia de la Unión Europea

TLD	dominio de nivel superior
TPP	Acuerdo de asociación transpacífico
TRIPS	Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio
TTIP	Asociación Transatlántica de Comercio e Inversión
UA	Unión Africana
UDRP	Política uniforme de resolución de disputas
UIT	Unión Internacional de Telecomunicaciones
UIT-D	Sector de Desarrollo de las Telecomunicaciones de la UIT
UIT-T	Sector de Normalización de las Telecomunicaciones
UMAP	Movilidad universitaria en Asia y el Pacífico
UNDP	Programa de las naciones unidas para el desarrollo
UNESCAP	Comisión Económica y Social de las Naciones Unidas para Asia y el Pacífico
UNODC	Oficina de Naciones Unidas contra la Droga y el Delito
UNTOC	Convención contra la Delincuencia Organizada Transnacional
UPC	Códigos Universales de Producto
US(A)	EE.UU. (de América)
VCR	Videograbadora
VoIP	voz sobre protocolo de Internet
VPN	red privada virtual
W3C	Consorcio World Wide Web
WiMax	Interoperabilidad para el Acceso a Microondas
WLAN	redes de área local inalámbricas
WML	Lenguaje de Marcado Inalámbrico
WTSA	Asamblea Mundial de Normalización de las Telecomunicaciones (UIT)
www	world wide web
XHTML	eXtensible HTML
XML	eXtensible markup language
ZB	zettabytes
ZB	zettabytes

Para obtener una lista más completa de siglas, inicialismos, y abreviaturas utilizadas en la jerga de la gobernanza de Internet, consulte el Glosario de Acrónimos de DiploFoundation, disponible también en español, en https://www.diplomacy.edu/resources/books/internet-governance-acronym-glossary

Sobre el autor

El Dr. Jovan Kurbalija es el director fundador de DiploFoundation y está al frente de la Geneva Internet Platform. Como exdiplomático, su formación profesional y académica es el derecho internacional, la diplomacia, y la tecnología de la información. En 1992, creó la Unidad para la Tecnología de la Información y la Diplomacia en la Academia Mediterránea de Estudios Diplomáticos en Malta. Tras más de diez años de capacitación, investigación, y publicaciones, en 2002 la Unidad evolucionó para convertirse en DiploFoundation.

Desde 1994, el Dr. Kurbalija da cursos sobre el impacto de las TIC y la Internet en la diplomacia y la gobernanza de Internet. Actualmente, es profesor invitado en el Colegio de Europa de Brujas, Bélgica, y en la Universidad de San Galo, Suiza. Se desempeñó como profesor en la Academia Mediterránea de Estudios Diplomáticos en Malta, la Academia Diplomática de Viena en Austria, el Instituto Holandés de Relaciones Internacionales (Clingendael), el Instituto Universitario de Altos Estudios Internacionales y Desarrollo en Ginebra, Suiza, la Escuela Superior del Sistema de aprendizaje a personal de Naciones Unidas en Torino, Italia, y la Universidad del Sur de California, en Los Ángeles. Visualizó y dirige, desde 2005, el Programa de Construcción de Capacidades de la Gobernanza de Internet de DiploFoundation. Los principales intereses de investigación del Dr. Kurbalija incluyen el desarrollo de un régimen internacional para Internet, el uso de Internet para la diplomacia y las negociaciones modernas, y el impacto de Internet en las relaciones internacionales modernas.

Jovan ha publicado y editado numerosos libros, artículos, y capítulos, incluidos: *The Internet Guide for Diplomats, Knowledge and Diplomacy, The Influence of IT on Diplomatic Practice, Information Technology and the Diplomatic Services of Developing Countries, Modern Diplomacy,* y *Language and Diplomacy*. Fue coautor, junto con Stefano Baldi y Eduardo Gelbstein, de la *Information Society Library*, ocho volúmenes que cubren una amplia gama de desarrollos relacionados con Internet.

jovank@diplomacy.edu

INTRODUCCIÓN A LA GOBERNANZA DE INTERNET

Jovan Kurbalija

Introducción a la gobernanza de Internet brinda una revisión integral sobre los principales asuntos y actores de este campo. Escrito de una manera clara y accesible, complementado con gráficos e ilustraciones, este libro se centra en los aspectos técnicos, legales, económicos, socioculturales, de seguridad, desarrollo y derechos humanos de la gobernanza de Internet. Cuenta con una breve introducción, un resumen de las preguntas y controversias más importantes, y un estudio sobre los diferentes enfoques y opiniones para cada tema. Así, este libro ofrece un marco práctico para el análisis y el debate de la gobernanza de Internet.

Desde 1997, más de 3000 diplomáticos, especialistas informáticos, activistas de la sociedad civil, y académicos asisten a cursos de capacitación basados en los textos y enfoques que presenta este libro. En cada dictado de los cursos, el material se actualiza y mejora, haciendo de este libro un recurso didáctico particularmente útil para los estudios de introducción a la gobernanza de Internet.

9789993253310