LA GOBERNANZA DE INTERNET: LA TRAMPA DE LAS FORMAS[1]

CELE
Autor: **Carlos Cortés**

Septiembre 2014

CELE
Centro de Estudios en Libertad de Expresión y Acceso a la Información

1 Este documento fue elaborado por Carlos Cortés, investigador del iLei en el CELE. La investigación contó con el apoyo de Juan Diego Castañeda.

RESUMEN

Este documento ofrece una visión crítica sobre la gobernanza de Internet pensada para la acción de la sociedad civil. La tesis general es que el debate alrededor de la gobernanza de Internet ha estado demasiado centrado en la gobernanza misma antes que en lo que implica.

La primera parte ubica la gobernanza de Internet como una configuración de poder y tecnología, y se refiere a los temas principales que la componen. La segunda parte aborda la noción de la participación plural de los actores (el modelo 'multi-stakeholder') y el rol del Estado. Finalmente, el tercer capítulo hace un comentario de cierre y ofrece las siguientes conclusiones y recomendaciones:

- La gobernanza de Internet, antes que el conjunto de instituciones y fórmulas multilaterales de discusión, es un espacio de disputa alrededor del control y la gestión de una tecnología.
- El estudio de la gobernanza de Internet debe abrirse a todos aquellos que ejercen poder en la red, sin importar el escenario en el que se encuentren.
- La gobernanza de Internet no es del todo útil para saber cómo gobernar Internet. Como marco de referencia para abordar problemas y para proponer soluciones desde la sociedad civil, parece insuficiente.
- Para avanzar en una aproximación nueva de la gobernanza de Internet es necesario desintegrar el concepto de Internet para abordar las tensiones que existen en ese espacio en diferentes frentes.
- La arquitectura de Internet es el elemento estructurador más relevante a la hora de analizar cómo estos balances se juegan en la práctica.
- Hasta hoy la sociedad civil ha promovido la fórmula del diálogo 'multi-stakeholder'. Sin embargo, los actores relevantes no están llegando a esos escenarios con la intención de reevaluar su posición de poder en la red.
- La sociedad civil debe elevarles a los actores interesados los costos de tomar decisiones a espaldas del interés público.
- Aceptar una visión heterogénea de la gobernanza de Internet pasa por que los Estados entiendan que su papel en la gestión y control de Internet varía según el contexto.

1. INTRODUCCIÓN

En 1983 Internet alcanzó la mayoría de edad. Fue en ese año cuando se implementó el protocolo TCP/IP, según el cual todos los datos en la red se dividen en paquetes y se transmiten por igual a los extremos de ésta. Con esta decisión técnica, la incipiente red militar y académica empezó a expandirse como una telaraña: cientos de redes encontraron caminos entre sí; miles de computadores comenzaron a conectarse.

Arpanet –el antepasado de Internet– era hasta entonces un jardín amurallado del que solo hacían parte unos pocos. Para los ingenieros el reto ya no era conectar computadores entre sí, sino lograr que redes distintas interactuaran sin necesidad de intervenirlas o configurarlas. Un cable, un módem, un ordenador, y listo. De ahí en adelante la red no pararía de desarrollarse: en 1989 vendría la invención del *World Wide Web*; en 1993 llegaría el primer navegador apto para gráficas y, dos años después, se privatizarían los puntos principales de conexión, dando lugar a la espina dorsal de la red (el *backbone*).[2]

Hoy, más de 30 años después, la estructura y densidad de Internet es mucho más sofisticada. De una población de aficionados y expertos en sistemas, pasamos a tener aproximadamente tres mil millones de 'ciudadanos' de 194 países.3 De una red dedicada principalmente al intercambio de correos electrónicos y la navegación de páginas web, pasamos a una de servicios de voz, 'streaming' de video y alojamiento de archivos en la nube. De una red compuesta por computadores, pasamos a una interconectada por teléfonos móviles, tabletas, radios y hasta automóviles. De una red compuesta por pocos actores en medio de acuerdos básicos, llegamos a una inmersa en complejas transacciones comerciales. Y, finalmente, de una red desarrollada y manejada por particulares, vamos desembocando en una donde los Estados también quieren ser protagonistas.[4]

Es en este contexto donde se discute el qué y el cómo de la gestión y el control de Internet: la gobernanza de Internet. No resulta fácil demarcar sus límites, pero tal vez sí sea más sencillo entender lo que está en juego. Alrededor de la pregunta de cómo se gobierna el entorno digital está la respuesta a temas como la protección de la privacidad en línea y el anonimato de los usuarios, el rol de las empresas privadas que controlan la infraestructura de Internet, las pretensiones de los Estados nacionales, la responsabilidad de los intermediarios y, claro, la libertad de expresión.

Teniendo en cuenta que existen decenas de libros, manuales y guías sobre gobernanza de Internet, escribir algo más sobre el tema puede parecer redundante. Partiendo de ese supuesto, antes que engrosar la lista de estudios descriptivos, este documento intenta ofrecer una visión crítica pensada, sobre todo, para la acción de la sociedad civil.

La primera parte ubica la gobernanza de Internet como una configuración de poder y tecnología, y se refiere a los temas principales que la componen. La segunda parte aborda la noción, transversal a la gobernanza de Internet, de la participación plural de los actores (el modelo 'multi-stakeholder') y el rol del Estado. Finalmente, el tercer capítulo ofrece algunas conclusiones y propuestas.

2 Cfr. Hefner, K. When Wizards Stay Up Late: The Origins of the Internet. Simon & Schuste, 1998.

3 Cfr. 'ITU releases 2014 ICT figures. Mobile-broadband penetration approaching 32 per cent. Three billion Internet users by end of this year'. Comunicado de prensa. Disponible en: http://www.itu.int/net/pressoffice/press_releases/2014/23.aspx#.U-ZRD4BdVg5 (consultado el 18 de agosto de 2014).

4 Cfr. Yoo, C. The Dynamic Internet: How Technology, Users, and Businesses Are Transforming the Network. AEI Press, 2012.

2. GOBERNANZA DE INTERNET: CONFIGURACIONES DE PODER Y DE TECNOLOGÍA

En 1999 Lawrence Lessig enunció el famoso postulado de "*el código es ley en Internet*"[5] para describir la manera en que las reglas informáticas determinan el comportamiento del individuo en el entorno digital. No es el único factor influyente. Para Lessig, al código se suman las leyes, las normas sociales y el mercado. Cohen respondió críticamente a esta teoría: para ella, es errado enunciar estos factores como entes autónomos desplegados o promovidos por actores desinteresados. La configuración del entorno digital, afirma, está inscrita en nuevas formas de ordenamiento social de la emergente sociedad de la información. En ese sentido, las fuerzas que describe Lessig hacen parte de agendas promovidas por distintos actores.[6]

El propio Lessig complementó y contextualizó su teoría en escritos posteriores.[7] Pero más allá de ese debate, acá es posible ubicar un punto de partida para abordar la gobernanza de Internet. Las fuerzas económicas y políticas, el mercado y las comunidades de usuarios, ejercen una influencia directa en el diseño y administración de cualquier sistema –incluido Internet–. La tecnología "*incrusta y está incrustada en prácticas sociales, identidades, normas, convenciones, discursos, instrumentos e instituciones*".[8] Ese campo de disputa es lo que conocemos como la gobernanza de Internet.

Puppis asocia el concepto de 'gobernanza' con procesos ciudadanos de participación y deliberación que surgen ante las crecientes dificultades de los Estados para regular los problemas sociales, la fragmentación de poder y de conocimiento, y las nuevas autonomías de distintas partes de la sociedad.[9] En ese mismo sentido, Iosifidis plantea que la diferencia entre gobierno y gobernanza radica en la fuente que ejerce el poder. El Estado es el principal actor en la acción de gobernar, mientras que la gobernanza involucra a varios agentes e implica un poder compartido.[10]

No vale la pena detenerse ahora a buscar una definición exacta de gobernanza –que por demás es esquiva–. Para efectos prácticos, entendemos que se trata de la gestión y el control de una actividad en la que participan múltiples actores –públicos y privados– con intereses contrapuestos. En ese sentido, la gobernanza de Internet "*involucra el diseño y la administración de las tecnologías necesarias para mantener el funcionamiento de Internet y la aplicación de políticas sustanciales alrededor de esas tecnologías*". En palabras de Mueller, "*es la etiqueta más simple, directa e inclusiva para hablar de las actuales disputas y deliberaciones sobre cómo debe coordinarse, administrarse y modelarse Internet para reflejar políticas*".[11] En la misma línea, Mathiason define la gobernanza de Internet como un problema por solucionar. El propósito, afirma, es asegurar que las funciones y los actores que las ejecutan se comporten de tal manera que la red pueda funcionar. [12]

Entender la gobernanza de Internet como un juego de equilibrios de poder y un fenómeno social permite alejarse de una visión meramente institucional (sin que ello implique desecharla). Según Van Eeten y Mueller, el área de investigación de este tema ha estado fuertemente atada al estudio de entidades o espacios formales –como ICANN, la Cumbre Mundial sobre la Sociedad de la Información o el Foro de Gobernanza de Internet– donde no necesariamente 'sucede' la gobernanza. "*Estudiar una institución centralizada es mucho más conveniente que tener que identificar y estudiar la amplia gama de procesos desarticulados, desordenados y distribuidos globalmente, que producen la gobernanza*", explican los autores.[13]

La espina dorsal de la gobernanza de Internet es su configuración tecnológica, no solo porque moldea el entorno digital y condiciona la conducta de los usuarios, sino también porque determina el poder de los distintos actores. Se trata de una relación simbiótica: la configuración tecnológica distribuye poder y el poder determina configuraciones tecnológicas.[14] En palabras de Latour, la arquitectura técnica es política por otros medios,[15] exenta de deliberación democrática y proclive a

5 Cfr. Lessig, L. Code and Other Laws of Cyberspace. Basic Books, 1999.
6 Cfr. Cohen, J. Configuring the Networked Self: Law, Code, and the Play of Everyday Practice.
7 Ver, por ejemplo, Lessig, L. Code 2.0. Basic Books, 2006.
8 Jasanoff, Sheila. 'The Idiom of Co -Production'. En: Sheila Jasanoff , ed., States of Knowledge: The Co-Production of Science and Social Order, London : Routledge, 2004, p. 3. Citado en De Nardis, Laura. The Global War for Internet Governance. Yale University Press, 2014, p. 6 (traducción informal).
9 Cfr. Puppis, M. 'Media Governance: A New Concept for the Analysis of Media Policy and Regulation'. En: Communication, Culture & Critique 3, 2010, p. 134-149.
10 Cfr. Iosifidis, P. Global Media and Communication Policy. Palgrave, Macmillan, 2011.
11 Mueller, M. Network and States. The Global Politics of Internet Governance. MIT Press, 2010, p.9 (traducción informal).
12 Cfr. Mathiason, J. Internet Governance. The New Frontier of Global Institutions. Routledge Global Institutions, 2009.
13 Van Eeten, M.; Mueller, M. Where is the Internet Governance? New Media Society, 2013, 15, p. 729 (traducción informal).
14 Cfr. Feenberg, Andrew. Between Reason and Experience. Essays in Technology and Modernity. MIT, 2010.
15 Cfr. Latour, B. The Pasteurization of France. Harvard University Press, 1998. Citado en: Musiani, F. 'Network Architecture as Internet Governance'. Internet

fenómenos de dependencia (*path-dependency*) y consolidación (*lock-in*).

Alrededor de la arquitectura de la red se desarrolla entonces la gobernanza, cuyos debates pasan tanto por la forma como por el fondo: ¿quién toma las decisiones sobre el funcionamiento y la administración de Internet?, ¿cómo decide? Antes de estas preguntas hay otras, igualmente complicadas, de carácter metodológico: ¿a qué funciones nos referimos?, ¿existe una lista taxativa?, ¿cuáles son los temas de la gobernanza?

"*El propio significado del término 'gobernanza de Internet' varía a partir de los antecedentes y objetivos de quien lo invoca*", afirman Brousseau y Marzouki. "*El resultado son muchas ambigüedades y malentendidos a la hora de definir el terreno de juego y los elementos*".[16] A pesar de este nivel de subjetividad, es posible identificar temas recurrentes, aunque no necesariamente excluyentes: (i) recursos críticos de Internet; (ii) estándares técnicos; (iii) acceso e interconexión; (iv) seguridad, y (v) regulación de contenidos y propiedad intelectual.[17]

Frente a la gobernanza de cada uno de ellos hay visiones diametralmente opuestas. Mientras algunos actores ven Internet como un espacio público donde deben favorecerse el interés general, los derechos humanos y el debate democrático, otros lo entienden como un espacio para innovación e intercambio comercial, sujeto a las leyes del mercado y la libre competencia.[18] Por supuesto, en medio de esas posiciones hay todo tipo de planteamientos.

En el siguiente aparte de este capítulo explicaremos estos temas. Es importante reiterar el objetivo de este documento. Cada uno de estos asuntos es complejo y merece un estudio aparte. Para empezar, en la literatura citada hay un amplio menú para hacerlo. El propósito nuestro, más bien, es ubicar al lector en estos temas para plantear después un debate general sobre la gobernanza de Internet.

a. Recursos críticos de Internet

Los recursos críticos de Internet son una serie de elementos virtuales indispensables para el funcionamiento de la red. Las direcciones de protocolo de Internet (*IP addresses*), el Sistema de Nombres de Dominio (*Domain Name System*) y los Sistemas Autónomos (*Autonomous Systems*), son ejemplos de estos recursos.[19]

Las direcciones IP sirven para identificar cada dispositivo que se conecta a Internet con el fin de que el sistema sepa a dónde debe dirigir los datos que el usuario solicita. Debido a su naturaleza, el primer sistema en funcionamiento (IPv4) puede asignar aproximadamente 4,3 billones de direcciones únicas. Hoy ese número se está quedando corto, por lo que se busca implementar un sistema (llamado IPv6) que permita una mayor cantidad de direcciones.

Por su parte, el sistema de nombres de dominio surge de la necesidad de usar nombres asequibles para identificar direcciones IP en vez de asociarlas a una extensa retahíla de números. Así, en vez de tener que teclear '72.14.192.0' –un número de difícil recordación– se asocia éste a una dirección en texto. En ese caso, www.google.com. El sistema evolucionó de una simple lista en un archivo de texto a una base de datos distribuida en varios servidores.

Los nombres de dominio cuentan con distintas 'extensiones' que acompañan la identificación inicial: desde el paradigmático '.com' hasta el '.aero', pasando por '.edu, '.org', '.info', entre otros. Los nombres de dominio están entonces divididos en subgrupos, que en su primer orden se denominan *Generic Top Level Domains* o gTLD. La idea es que todos los nombres de dominio posibles se inserten en uno de esos grupos, cuya administración se entrega a organizaciones privadas, que a su vez permiten que otras empresas vendan a particulares el registro de dominios concretos. También existen TLD relacionados con países, por ejemplo, '.co' para Colombia o '.ar' para Argentina.

Finalmente, los sistemas autónomos son números binarios que se asignan a cada operador de la red y que, como las direcciones IP, son únicos e indispensables para permitir la conexión entre redes. En otras palabras, es un identificador que se publica o se da a conocer a otros operadores para que sus redes sepan de la existencia de las otras y se interconecten.

Policy Review, Vol. 2, Issue .4

16 Brousseau, E.; Marzouki, M. 'Internet governance: old issues, new framings, uncertain implications'. En: Governance, Regulations and Powers on the Internet. Cambridge University Press, 2012, p. 368 (traducción informal).

17 Cfr., además de las obras ya citadas, De Nardis, L.; Raymond, M. 'Thinking Clearly about Multistakeholder Internet Governanca'. Paper Presented at Eighth Annual GigaNet Symposium. Bali, Indonesia, 2013.

18 Cfr. Op. Cit. Brousseau, E.; Marzouki, M.

19 Para una explicación más detallada de los DNS y el sistema de direcciones IP, ver: Bertoni, E.; Grimani, A. 'Nombres de dominio: una expresión que merece ser protegida. Recomendaciones y sugerencias para administradores locales de América Latina y el mundo'. En: Internet y derechos

Estos recursos se asignan de manera individual y específica a cada persona, dispositivo o red que se conecta a Internet. Así, no puede haber dos computadores con la misma dirección IP, dos personas que puedan controlar a la vez un nombre de dominio –como www.wikipedia.org– o dos sistemas autónomos con el mismo identificador. Esta asignación de recursos requiere, por supuesto, de algún tipo de coordinación,[20] que hoy en día ejerce la Autoridad de Números Asignados en Internet (IANA, por su nombre en inglés). La IANA es un departamento de –o un conjunto de funciones a cargo de– la Corporación de Internet para la Asignación de Nombres y Números (ICANN, por su nombre en inglés).

A través de IANA, ICANNN se encarga de dirigir y autorizar el uso de nombres de dominio y de direcciones IP. Pero no todas las funciones las ejerce directamente. El Sistema de Nombres de Dominio –que, como dijimos, permite encontrar una dirección en un TLD en particular– se encuentra en trece servidores raíz (*root servers*) administrados por empresas o entidades distintas. Por otra parte, cada TLD es manejado también por una empresa u organización diferente, a partir de una base de datos llamada 'Registro de nombre de dominio', (*Domain Name Registry*). Estos actores privados puede autorizar a empresas, conocidas como registradores (*registrars*), para que comercialicen los registros entre particulares.

Por último, ICANN delega la asignación de direcciones IP a entidades llamadas registries –también conocidas como RIR (*Regional Internet Registry*). Existen cinco y cada una se encarga, en una región del mundo, de asignar números en bloque a prestadores de servicio de Internet para que éstos puedan ofrecerlos a sus clientes.

Existen varios problemas frente a los recursos críticos. Mencionemos acá tres de ellos. El primero se refiere al mercado de los gTLD. A diferencia de las direcciones IP o los Sistemas Autónomos, y de acuerdo con lo explicado arriba, los gTLD se pueden comprar y vender como cualquier producto comercial. Esto implica que entre más gTLD haya, más comercialización y productos habrá. Esto pone en jaque a las empresas dedicadas a defender los derechos de propiedad intelectual. Para estos actores resulta inconveniente que haya demasiados gTLD, toda vez que implica más frentes abiertos –todos los dominios relacionados con su marca– para defender.[21] Pero no solo los particulares tienen intereses económicos en la materia sino que también para ICANN representa un beneficio, pues cobra USD 185.000 por estudiar la posibilidad de crear y entregar al solicitante un nuevo gTLD.[22]

Por otro lado está la cuestión de la pluralidad en el lenguaje de los TLD. Los caracteres con los que se escriben se ajustan al estándar estadounidense para el intercambio de información (ASCII, en inglés). Por esta razón, caracteres en otros idiomas –como la letra 'ñ'– no hacen parte de los TLD. Esto ha generado una tensión entre países y grupos culturales para quienes Internet debe reflejar la pluralidad de lenguas distintas al estándar ASCII. ICANN ha estudiado el problema balanceando ventajas y desventajas de incluir otros caracteres dentro de los TLD.[23] Por ahora, autorizó el registro de 31 gTLD en caracteres en árabe, chino y ruso.[24]

Finalmente, el problema de las direcciones IP, también relacionado con el asunto de los contenidos, que veremos más adelante. En ocasiones, titulares de copyright en Estados Unidos logran rastrear dónde terminan descargadas sus obras gracias a las direcciones IP. Basados en este dato, buscan que los jueces autoricen la entrega de los datos personales del usuario al que corresponde ese identificador. Por ahora las autoridades de ese país no han aceptado esa pretensión, y consideran que la dirección IP no equivale a la identidad de un supuesto infractor.[25] En últimas, los titulares de copyright buscan que este recurso crítico puede usarse como una herramienta de control frente al uso no autorizado de sus contenidos.

b. Establecimiento de estándares técnicos

Así como las vías públicas requieren reglas para que cada automóvil pueda llegar seguro del punto A al punto B, en Internet se emplean reglas –llamadas protocolos– para recibir y transmitir información y, en general, para que el sistema funcione. La principal preocupación que subyace a la creación de protocolos es la interoperabilidad, es decir, la posibilidad de que todos los operadores y aplicaciones del sistema funcionen bajo las mismas reglas.

20 Cfr. Op. Cit. De Nardis, 2014.
21 Cfr. Mueller, M. Ruling the Root. MIT Press, 2002.
22 Cfr. ICANN. Applicant Guidebook. Versión 2012-06-04, p.1-42.
23 Cfr. ICANN. 'Discussion Paper on Non-ASCII Top-Level Domain Policy Issues'. Disponible en: http://archive.icann.org/en/committees/idn/non-ascii-tld-paper-13jun02.htm (consultado el 15 de agosto de 2014).
24 Cfr. ICANN. 'Delegated strings'. Disponible en: http://newgtlds.icann.org/en/program-status/delegated-strings (consultado el 15 de agosto de 2014).
25 Cfr. Torrentfreak. 'Judge: IP-Address is Not a Person and Can't Identify a Bittorrent Pirate', 24 de marzo de 2014. Disponible en: https://torrentfreak.com/ip-address-not-person-140324/ (consultado el 18 de agosto de 2014).

El protocolo más importante para Internet se denomina TCP/IP (*Transmission Control Protocol/Internet Protocol*), y es el que indica para dónde van los datos, cómo se dividen en paquetes y cómo deben rearmarse en su lugar de destino. Además de este, existen otros como SMTP, para transmisión de emails, FTP para transmisión de archivos y HTTP, para la transmisión de páginas web.[26]

El diseño de protocolos de Internet está a cargo del Grupo de Trabajo de Ingeniería de Internet (IETF por su nombre en inglés), una organización informal de personas con interés y conocimiento técnico suficiente para proponerle a sus iguales estas reglas técnicas. Por su parte, el World Wide Web Consortium (W3C) es el organismo encargado de determinar estándares para el funcionamiento de la web.

Un debate relevante frente a la definición de estándares tiene que ver con la forma como éstos afectan el derecho a la privacidad en el entorno digital. Por ejemplo, el TCP/IP –el protocolo básico de la red– impone el trato igualitario de paquetes y datos y desarrolla el principio de 'extremo a extremo', lo cual, en principio, resulta más amigable para la privacidad de los usuarios. De manera similar, pero en un nivel distinto de jerarquía en la red, el protocolo para el intercambio de archivos BitTorrent está diseñado para evitar la conservación de registros de direcciones IP, haciendo más difícil la persecución de quienes lo usan. Las características de estos protocolos, y en especial aquellos que configuran la arquitectura original de Internet, son objeto de críticas y presiones. Por distintas razones –seguridad, *copyright*, prevención del crimen– desde muchas orillas se propone reformarlos para que resulte más fácil identificar a los usuarios.

Por otro lado, recientemente el W3C anunció que incluiría dentro del estándar web la protección de contenidos por medio de DRM (*Digital Rights Management*), una serie de códigos informáticos que evitan la copia, modificación o usos no autorizados de cualquier contenido protegido por *copyright*. Los DRM, en general, someten los contenidos a un control casi perfecto por parte de sus propietarios, mucho más allá de lo que permiten las leyes sobre derecho de autor.[27] Por esa razón, el anuncio de W3C levantó muchas críticas, que, en síntesis, apuntan a un desmedro del dominio público y los usuarios en favor de una industria en particular.[28]

c. Acceso e interconexión

Internet es una red de redes. Esto quiere decir que su carácter global –esa economía de escala que la define– depende de que los operadores de cada red lleguen a acuerdos para interconectarse. Para el efecto, los prestadores del servicio de red tienen tres opciones generales: (i) vender la interconexión a operadores de menor tamaño y conectarse, en principio de forma gratuita, a otras redes de su mismo nivel; (ii) comprar a las redes de primer nivel la interconexión y venderla a los de tercer nivel, o (iii) sólo comprar la interconexión al segundo nivel para proveerla a sus clientes.

No obstante, los incentivos para mover datos y los distintos tipos de aplicaciones han propiciado la aparición de nuevos intermediarios y servicios. Hoy existen, por ejemplo, los puntos de intercambio de tráfico (*Internet Exchange Points,* o IXP), las redes de distribución de contenidos (*Content Delivery Networks*) y las 'granjas de servidores', que al igual que las redes más tradicionales, buscan acuerdos con los prestadores del servicio de Internet para llevar el contenido al usuario final.[29]

Más allá de los problemas y retos técnicos, la complejidad de la red importa en términos de gestión y administración. Los acuerdos entre todos estos actores son privados; se han llevado a cabo por fuera de contextos normativos tradicionales, y están motivados y estructurados por intereses económicos particulares antes que mandatos técnicos o provisiones de interés público. El primer interés de ellos es ofrecer servicios exclusivos –mejor remunerados y de calidad más alta– para usuarios con expectativas comerciales muy claras. Y aunque muchas de esas prácticas puedan satisfacer a un público determinado, ponen en riesgo la unidad y carácter común de la red.[30]

La solución de estos problemas es sumamente compleja. Algunos expertos sugieren la creación de un régimen público de

26 Para una explicación básica de los protocolos de Internet y, en particular, del TCP/IP, vea: Cortés, C. 'La neutralidad de la red: la tensión entre la no discriminación y la gestión' y 'Vigilancia en la red: ¿qué significa monitorear y detectar contenidos en Internet'. En: Op. Cit. Internet y derechos humanos. Aportes para la discusión en América Latina.

27 Cfr. Cohen, J. 'Pervasively Distributed Copyright Enforcement'. Georgetown Public Law and Legal Theory Research Paper No. 892623. The Georgetown Law Journal, Vol. 95:1, 2006, p. 2 y ss.

28 EFF. 'Lowering Your Standards: DRM and the Future of the W3C'. Disponible en: https://www.eff.org/deeplinks/2013/10/lowering-your-standards (consultado el 18 de agosto de 2014).

29 Cfr. Op. Cit. Yoo, C.

30 Cfr. Chapin, L. 'Interconnection and peering among Internet Service Providers'. Interisle White Paper, 2005.

interconexiones –como las autopistas y vías de un país– o la imposición de tarifas estándar de intercambio de tráfico para evitar prácticas anti-competitivas. Estas propuestas, sin embargo, no han logrado dar cuenta de la cantidad de actores emergentes, la escala y diversidad de los acuerdos privados existentes, y el tipo de solución aplicable. En últimas, un temor fundado en toda la regulación de la tecnología y la innovación, es imponer una solución que, como una camisa de fuerza, atente contra la misma evolución de la red.[31]

d. Seguridad

De la seguridad de la red dependen los operadores y los usuarios. Los 'ataques de denegación de servicio' (conocidos como *Denial of Service Attacks*, *DoS* o *DDoS*), el robo de información, la suplantación de identidad, el uso de 'spyware, y una larga lista de riesgos, son una realidad en el entorno digital. De la mano con la expansión de la red y la llegada de nuevos servicios, vienen también los problemas en materia de seguridad.

La seguridad de Internet toca una lista innumerable de asuntos: tiene que ver con consideraciones sobre integridad de datos, autenticación y confidencialidad de usuarios, prevención de accesos no autorizados, detección y respuesta ante ataques informáticos, confianza de los usuarios para hacer pagos en línea y la amplia agenda de la seguridad nacional de los Estados.[32]

El sector comercial –del que también hacen parte las empresas que ofrecen las soluciones a estos riesgos– suelen ser reiterativas al hablar de la cantidad de dinero que se pierde por cuenta de la inseguridad en línea.[33] Y aunque el problema existe y no debe ser subestimado, el discurso de la seguridad, al igual que el del *copyright*, es sobre todo favorable a los intereses de ciertos jugadores. Las arquitecturas de control –como planteábamos antes– tienen detrás una agenda de distribución de poder y determinación de conductas.[34]

La seguridad en la red ha sido tema de discusión en las instituciones formales de la gobernanza de Internet.[35] Las soluciones varían tanto en términos técnicos como políticos. Están, por ejemplo, los grupos nacionales de respuesta rápida (CERT, por su nombre en inglés), los certificados de autenticidad de servicios y aplicaciones, y las propuestas para mejorar la seguridad en el núcleo del diseño de la red (protocolos de seguridad como DNSSec o IPSec).

Desde el punto de vista de la gobernanza de Internet, el problema básico –como muchos en esta área– es la dificultad para coordinar a los grupos de interés. Los Estados tradicionalmente han sido responsables de mantener la seguridad de sus ciudadanos, pero hoy se encuentran actuando como iguales dentro de un grupo de actores no estatales, acordando reglas y métodos más allá de su mandato legal y sus posibilidades prácticas.[36]

La posibilidad de centralizar el control en el Estado tampoco parece viable. La configuración abierta y descentralizada de Internet y su incorporación social dispersa y múltiple, impone un camino igualmente distribuido en materia de seguridad. Que los gobiernos impulsen regulaciones concentradas y centralizadas alrededor de su poder punitivo no solo resulta poco práctico e ineficiente, sino que, al igual que en otros casos, puede propiciar cambios estructurales negativos en el entorno digital, en detrimento de la libertad de expresión, la privacidad y otros derechos fundamentales.[37]

e. Regulación de contenidos y propiedad intelectual

No existe un tema sobre el cual haya mayor expectativa que la regulación de los contenidos en línea. Tanto los Estados como los actores privados enfrentan en Internet el riesgo de la pérdida de control frente a qué contenidos intercambian los usuarios, para qué los usan y cómo lo hacen. Los motivos varían de la misma forma que las estrategias. Por razones políticas, comerciales o simplemente estratégicas (que no son tema de este documento), unos y otros recurren a la tecnología –apoyada por la regulación o los acuerdos entre particulares– para ponerle cerrojos a la red.

Existen muchas tecnologías que permiten bloquear o filtrar contenidos: la inspección profunda de paquetes, que permi-

31 Cfr. Faratin, P. et al. 'The Growing Complexity of Internet Interconnection'. Communications & Strategies, no. 72, 4th quarter 2008. Ver también, Op. Cit. Yoo, C.
32 Cfr. Doria, A. 'What do the Words "Internet Security" Mean?'. En: The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment. Wolfgang Kleinwächter, 2007.
33 Cfr. Brenner, J. 'Eyes wide shut: The growing threat of cyber attacks on industrial control systems'. Bulletin of the Atomic Scientists 69(5) 15–20. 2013.
34 Cfr. Op. Cit. Cohen, 2012.
35 Cfr. Gupta, A.; Samuel, C. 'A Comprehensive Approach to Internet Governance and Cybersecurity'. Strategic Analysis, Vol. 38, No. 4, 588–594. 2014.
36 Mueller, Milton; Schmidt, Andreas y Kuerbis, Brenden. Internet Security and Networked Governance in International Relations. International Studies Review. 15, 86–104. 2013.
37 Cfr. Deibert, R. Black Code: Inside the Battle for Cyberspace. McClelland & Stewart, 2013.

te discriminar el destinatario, el emisor o el contenido de la transmisión; el bloqueo de dominios, que impide la consulta de un sitio web en particular; la inhabilitación de sitios o servicios por medio de ataques de denegación del servicio, o la instalación de filtros en puntos de acceso de la red, como el prestador del servicio o el 'ama de llaves' de un grupo de computadores.[38]

El control técnico puede tener como fuente una ley, un tratado internacional –como veremos en el siguiente tema– o un acuerdo privado. Estas medidas, además, suelen combinarse con imposiciones operativas a los intermediarios, como son las licencias de funcionamiento o los registros obligatorios (para, por ejemplo, tener un ciber-café).[39] Cuando el Estado no tiene poder directo sobre los medios técnicos que facilitan la conexión, como sucede en la mayoría de los casos, debe presionar los puntos donde pueda realizar un control efectivo. Esos puntos son los intermediarios de Internet, que prestan servicios de conexión (como Claro o Telmex), de información (Google o Yahoo!), de acceso a contenidos (YouTube), o de transacciones financieras (PayPal y bancos tradicionales).[40]

También se pueden imponer usos de la tecnología –que en últimas consiguen el objetivo último de control del contenido– desde su fase de diseño. Es el caso de los DRM mencionados anteriormente, que imponen, por ejemplo, que un archivo de música o video solo pueda usarse en un dispositivo aprobado o por un tiempo fijo. Lo mismo sucede con el software que restringe ciertos usos en un computador, o los programas que supervisan la actividad del usuario con el propósito de que se ajuste a la actividad autorizada.[41]

Todo esto encuentra en la industria del *copyright* un ferviente promotor. Desde la Organización Mundial del Comercio (OMC) se vienen discutiendo tratados internacionales para que el uso de obras en el entorno digital quede reducido, como decíamos antes, únicamente a las modalidades que autorice el propietario. Recientemente se ha propuesto crear una regulación transnacional vía acuerdos comerciales, dentro de los que se destacan el Acuerdo Comercial Anti-Falsificación (ACTA, por su nombre en inglés) y el Acuerdo Estratégico Trans-Pacífico de Asociación Económica (TPP, también por su nombre en inglés).

De manera complementaria, diversos Estados han adoptado leyes para ofrecerle al titular del material un procedimiento expedito para retirar contenidos de Internet. La regulación pionera en la materia y modelo de muchas otras es el DMCA (*Digital Millenium Copyright Act*) de los Estados Unidos. Estos regímenes han suscitado críticas entre los usuarios de Internet y académicos, para quienes esas soluciones resultan desproporcionadas y contrarias al debido proceso y la libertad de expresión.[42]

Además de lo relacionado con las creaciones protegidas por *copyright*, también existe un pulso por intervenir la gestión de recursos en favor de los derechos de propiedad intelectual (lo cual también se relaciona con el primer literal de este capítulo). La principal fuente de tensión es la asignación de nombres de dominio. Éstos se registran en favor de quien primero los solicite, un método al parecer eficiente en vista del volumen de peticiones que se formulan a diario.[43] Esto ha suscitado el descontento de los titulares de marcas que llegan tarde para registrar un dominio en particular. Por ejemplo, un particular registra www.mcdonalds.com en vez de la cadena de hamburguesas. Para resolver este problema, ICANN y la OMC diseñaron un sistema de resolución de disputas por nombres de dominio (UDRP, por su nombre en inglés) que busca defender al titular de una marca registrada y entregarle el nombre de dominio relacionado que otro haya registrado.[44]

El debate sobre el control de contenidos atraviesa todos los temas de la gobernanza de Internet. Es un medio y un fin en sí mismo, y se juega en múltiples escenarios y con diversos jugadores. Desde un punto de vista más general, su importancia reside en la fuente del control y la manera como lo instrumentaliza. Las tensiones suelen plantearse desde la perspectiva de los gobiernos y las leyes que impulsan con el propósito de controlar la información en línea. Sin embargo, los particulares, como subrogado del Estado o por cuenta propia, cumplen un papel igualmente relevante. Allí, los medios se vuelven invisibles: el código define la regulación del contenido, y la regulación de este contenido está en un contrato al que el usuario se adhiere con un clic.

38 Para una explicación completa de los diferentes medios técnicos para bloquear o filtrar contenidos, ver Murdoch, S.; Anderson, R. 'Tools and Technology of Internet Filtering'. En Deibert, Ronald, et al. Access Denied. MIT Press. 2008.

39 Cfr. Zittrain, J.; Palfrey, J. 'Internet Filtering: The Politics and Mechanisms of Control'. En, Ibidem.

40 Wu, Tim y Goldsmith, Jack. Who controls the Internet?. Illusions of a Borderless World. Oxford University Press. 2008. Ver también, Op. Cit. Cortés, C. 'Las llaves del ama de llaves.

41 Cfr. Zittrain, J. The Future of Internet and How to Stop It. Yale University Press, 2008.

42 Ver, entre otros, Lessig, L. Free Culture. Penguin Books. 2004; Vaidhyanathan, S. Copyrights and Copywrongs: The Rise of Intellectual Property and How it Threatens Creativity. NYU Press. 2003; Patry, W. Moral Panics and the Copyright Wars.Oxford University Press, 2009.

43 Cfr. Op. Cit. Mueller, M.

44 Ver, ICANN. Acerca de las disputas sobre nombres de dominio. Disponible en: https://www.icann.org/resources/pages/disputes-2013-07-17-es (consultado el 19 de agosto de 2014).

3. EL ROL DEL ESTADO, LOS PARTICULARES Y EL MODELO 'MULTI-STAKEHOLDER'

La mayoría de teorías acerca de la globalización suelen compartir el lugar común de la decadencia del Estado. Según éstas, la globalización socava la soberanía nacional y debilita la habilidad del gobierno para regular sus asuntos domésticos. Por otro lado, la globalización empodera a los actores no estatales debido a la reducción de costos de transacción entre fronteras y la posibilidad de trabajo en red.[45]

Estos presupuestos parecen diseñados a la medida de Internet, un fenómeno globalizado por naturaleza. Los Estados se ven limitados por su competencia territorial mientras que Internet no conoce fronteras; alrededor de Internet surgen nuevas formas de acción, colaboración y participación, mientras que los Estados tienen una capacidad limitada para intervenir; las comunicaciones son masivas y cambiantes, y la respuesta del Estado difícilmente se acopla a la velocidad y evolución de la tecnología.[46]

Para Drezner, si en algún escenario deberían evidenciarse a plenitud los efectos de esa globalización arrolladora, tendría que ser Internet. Por supuesto, ese no es el caso. Del ciber-entusiasmo del siglo pasado solo queda el recuerdo. Las palabras de Nicolás Negroponte –"*Internet no puede ser regulado. No es que las leyes no sean relevantes; es que el Estado-nación no es relevante*"–[47] o la declaración de independencia del ciberespacio que hiciera John Perry Barlow en 1996, son cosa del pasado.[48] Hoy en día la globalización de Internet pasa por muchos factores de poder, y la intervención del Estado se da por descontada.

Sería fácil concluir que las intervenciones de los gobiernos en Internet se dividen entre aquellos que son democráticos y aquellos que no. En un extremo están Estados Unidos, Alemania o Inglaterra, cuya intervención solo busca garantizar los derechos fundamentales y propiciar un entorno de confianza para las relaciones comerciales. En el otro aparecen países como China, Cuba o Irán, cuyo propósito de controlar la red no es otro que coartar las libertades individuales, vigilar a los ciudadanos y favorecer los intereses del partido en el poder.

El asunto, claro, es más complejo. Aunque es posible identificar gobiernos que abiertamente consideran Internet una amenaza para su estabilidad y proyecto político, entre el amplio grupo de países democráticos hay visiones contradictorias sobre el tipo de intervención estatal que amerita. Los contenidos ofensivos en línea, por ejemplo, han merecido respuestas regulatorias en países como Francia o Alemania, pero no en Estados Unidos. Los sitios de apuestas en línea, en cambio, no merecen ninguna respuesta en Europa, pero son sistemáticamente bloqueados en Estados Unidos.[49]

La regulación de los gobiernos funciona imponiendo costos y cargas, y en los casos más graves, también como un sello hermético. Lo cierto es que para intervenir en Internet, los Estados no han tenido que salir de sus fronteras; ha sido suficiente, como explicábamos anteriormente, con imponerles obligaciones a los intermediarios de Internet –las 'amas de llaves'– que se asientan en su territorio. De esta forma, con distintos niveles de éxito y dependiendo del país, se han hecho presentes en el entorno digital.[50]

Esto no quiere decir que ahora la red esté supeditada a la autoridad exclusiva de los Estados, o que los actores privados hayan perdido relevancia.[51] La realidad histórica, como explica De Nardis, es que "*la mayoría de funciones de la gobernanza de Internet no han sido de domino de los gobiernos, sino que han sido ejecutadas a través de órdenes privadas, diseño técnico y nuevas formas institucionales*".[52]

De este pulso entre gobiernos y particulares surge el modelo 'multi-stakeholder' –o de pluralidad de participantes interesa-

45 Cfr. Drezner, D. All Politics Is Global. Explaining International Regulatory Regimes. Princeton University Press, 2007.
46 Op. Cit. Mueller.
47 The Guardian. 'China Begins to Erect Second Great Wall in Cyberspace', 5 de febrero de 1996. Citado en: Op. Cit., Drezner, p. 94.
48 "*Gobiernos del Mundo Industrial, ustedes, gigantes cansados de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, les pido a ustedes, del pasado, que nos dejen en paz. No son bienvenidos entre nosotros. No tienen soberanía donde nos reunimos*". Barlow, J.P. A Declaration of Independence of Cyberspace. Disponible en: https://projects.eff.org/~barlow/Declaration- Final.html (consultado el 11 de agosto de 2014, traducción informal.
49 Cfr. Murray, A. The Regulation of Cyberspace. Control in the Online Environment. Routledge-Cavendish, 2007.
50 Cfr. Goldsmith, J.; Wu, T. Who Controls the Internet?: Illusions of a Borderless World. Oxford University Press, 2006. Para una explicación más detallada sobre los intermediarios en Internet, ver: Cortés, C. 'Las llaves del ama de llaves: la estrategia de los intermediarios en Internet y el impacto en el entorno digital'. En: Internet y derechos humanos. Aportes para la discusión en América Latina. CELE, Universidad de Palermo 2014.
51 Cfr. Op. Cit. Goldsmith, J.; Wu, T.
52 Cfr. Op. Cit. De Nardis, 2014, p. 11 (traducción informal).

dos– de la gobernanza de Internet. La Agenda de Túnez para la Sociedad de la Información lo describe en estos términos: "*Una definición de trabajo de la gobernanza de Internet es desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivos papeles, de principios, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y a la utilización de Internet*".[53]

De la Chapelle considera que la gobernanza 'multi-stakeholder' es necesaria para abordar asuntos transfronterizos como Internet, ya que permite apalancar estructuras diversas, como los gobiernos, las organizaciones de la sociedad civil, las empresas y las organizaciones internacionales. Dicho de otra forma, vuelve interoperables los distintos marcos de gobierno existentes. "*La gobernanza multi-stakeholder puede promover la democracia, enriquecer estructuras representativas existentes y empoderar a los ciudadanos en nuestro mundo interconectado e interdependiente*".[54]

El modelo 'multi-stakehoder' (y usamos el término en inglés a falta de una palabra precisa en español) se ha convertido en el referente del tema, el eje transversal a todas las áreas. Cuando se habla de gobernanza de Internet en espacios internacionales, es usual que enseguida se enuncie el modelo 'multi-stakehoder' como el camino a seguir. Una participación plural, horizontal y abierta –se dice– es la única forma de gobernar Internet.

De Nardis y Raymond critican que este modelo se presente como algo innovador e inherente a las particularidades de Internet, lo cual lo vuelve un fin antes que un medio. Así, el objetivo deja de ser la preservación de la interoperabilidad, estabilidad, seguridad y apertura de la red, para convertirse en la aplicación de la herramienta. Por otra parte, los autores consideran que el modelo 'multi-stakeholder' puede no ser el adecuado para cada área funcional de la gobernanza de Internet. Es decir, no es la 'talla única' para los problemas de administración y gestión de la red.[55]

El modelo 'multi-stakeholder' en este ámbito hace mucho énfasis en que existan lugares o instancias donde todos los actores estén convocados para hablar y proponer. Y entre más participación haya, mejor. Se parte de alguna forma del supuesto de que si el escenario está diseñado para hablar de gobernanza de Internet, habrá gobernanza de Internet. Pero, como suele evidenciarse en estos espacios, ni son todos los que están, ni están todos los que son.

Para Van Eeten y Mueller, esta perspectiva idealista "*ignora decisiones estratégicas que los actores hacen sobre en qué escenarios participarán y cuáles ignorarán, evitarán o boicotearán. Estos cálculos, basados en un interés propio básico, se vuelven extremadamente importantes cuando los actores tienen el control verdadero de un recurso y hay verdaderas pérdidas o ganancias como resultado de decisiones colectivas obligatorias*".[56]

Las definiciones sobre la gestión y el control de Internet se dan necesariamente en espacios donde las partes tienen algún incentivo para sentarse a interactuar y buscar acuerdos. Y en los escenarios 'multi-stakeholder' los convocados que tienen algún nivel de poder no llegan con la idea de jugárselo en una mesa de trabajo.[57]

El Foro de Gobernanza de Internet (IGF, por su nombre en inglés) es el escenario más conocido para el diálogo entre diversas partes interesadas. Sin embargo, la idea desde su concepción –recuerdan Van Eeten y Mueller– fue tener un lugar de intercambio donde no se pudieran tomar decisiones, impulsar mandatos o publicar conclusiones.[58] Para algunos, en esto consiste su atractivo: "*como nada saldrá de ahí, todos los asistentes pueden poner de lado por unos días sus pretensiones, alianzas, políticas formales e intereses, y simplemente hablar*".[59] El problema, evidente para muchos asistentes habituales a los IGF, es que las discusiones cándidas y espontáneas –salvo por algunos integrantes de la sociedad civil– terminan siendo elaboradas estrategias de relaciones públicas.

En abril pasado tuvo lugar en Brasil 'Net Mundial', la "*Reunión global de múltiples partes interesadas sobre el futuro de la gobernanza de Internet*".[60] Con el evidente interés del gobierno de Dilma Rousseff de introducir a su país entre los pesos pesados de este tema, la reunión convocó a 1.480 personas entre representantes de gobiernos, organismos multilatera-

53 Agenda de Túnez para la sociedad de la información. WSIS-05/TUNIS/DOC/6(Rev.1)-S, 2006. Disponible en: https://www.itu.int/wsis/docs2/tunis/off/6rev1-es.html (consultado el 11 de agosto de 2014).
54 De La Chapelle, B. 'Multistakeholder Governance: Principles and Challenges of an Innovative Political Paradigm'. En: MIND, Multistakeholder Internet Dialogue. Collaboratory Discussion Paper Series No. 1, 2011, p. 9 (traducción informal).
DeNardis, Laura (2014-01-14). The Global War for Internet Governance (p. 265). Yale University Press. Kindle Edition.
55 Cfr. Op. Cit., De Nardis, L.; Raymond, M.
56 Op. Cit. Van Eeten y Muller, p. 728 (traducción informal).
57 Cfr. Op. Cit., Van Eeten y Mueller.
58 Cfr. Ibidem.
59 Pacific Politics. 'Talking Shop', octubre de 2013. Disponible en: http://pacificpolitics.com/2013/10/talking-shop/ (consultado el 18 de agosto de 2014).
60 Ver www.netmundial.br (consultado el 18 de agosto de 2014).

les, empresas y sociedad civil. A diferencia del IGF, la conclusión de 'Net Mundial' fue un documento 'multi-stakeholder' que abarca todas las áreas relacionados con Internet. En particular, manifiesta que "*las decisiones sobre gobernanza de Internet en ocasiones se toman sin la participación significativa de todos los actores relevantes. Es importante que la toma de decisiones y formulación de políticas 'multi-stakeholder' mejore para asegurar una participación completa de todas las partes interesadas*".[61]

El documento fue objetado por 27 organizaciones de la sociedad civil, para quienes el resultado de la conferencia no refleja preocupaciones clave como la neutralidad de la red, la vigilancia masiva o la protección de la libertad de expresión.[62] En otras palabras, ese grupo manifiesta lo que el mismo documento había identificado como un problema: la falta de participación de ellos como actores de relevantes. Al parecer, varios gobiernos, entre ellos el de Estados Unidos, dieron un pulso para que varios de estos puntos estuvieran débilmente presentes en la versión final.[63]

La representación de la sociedad civil en el modelo 'multi-stakeholder' adolece además de una contradicción interna, y es la diferencia de visión entre las organizaciones más cercanas a los movimientos de derechos humanos y aquellas vinculadas a la comunidad técnica. La aproximación de esta última suele seguir el esquema inicial de desarrollo de la red, aún presente en algunas de las instituciones que definen estándares y recursos: autorregulación, consenso y permanencia de los principios y valores base de Internet. Por su parte, las organizaciones con un enfoque más político y legal, plantean discusiones amplias en términos del ejercicio de derechos fundamentales y controles democráticos. A pesar de que existen objetivos comunes en muchos de estos grupos, las expectativas y metas divergen en muchos puntos.[64]

Un último problema del modelo 'multi-stakeholder' se relaciona con la causa a la que puede terminar sirviendo. En muchos escenarios, las demandas de participación amplia hacen parte de una crítica al poder de Estados Unidos en la administración de ciertas funciones de la red –como se vio anteriormente–. En este sentido, para De Nardis "*las aproximaciones multi-stakeholder que buscan la promoción de la democracia pueden convertirse en una carrera por el más bajo común denominador sobre qué es un valor democrático aceptable*".[65] Al final del día, un modelo con una pluralidad mayor de participantes podría abrirle campo a países como Rusia o China para que –siguiendo sus valores democráticos y usando su músculo político– promuevan una visión de Internet ajena a la que de manera preponderante tiene la sociedad civil, al menos en América Latina.

61 Net Mundial. 'Net Mundial Multistakeholder Statement', abril de 2014 (traducción informal).
62 Cfr. Best Bits.'Civil society closing statement at NETmundial 2014'. Disponible en: http://bestbits.net/netmundial-response/ (consultado el 18 de agosto de 2014). Otras organizaciones, como la Asociación para el Progreso de las Comunicaciones , destacaron avances que se lograron en la reunión. Ver, https://www.apc.org/en/node/19224/ (consultado el 19 de agosto de 201).
63 Cfr. Tech Liberation. 'NETmundial wrap-up', abril 25 de 2014. Disponible en: http://techliberation.com/2014/04/25/netmundial-wrap-up/ (consultado el 18 de agosto de 2014).
64 Cfr. Op. Cit., Brousseau, E.; Marzouki, M.
65 Op. Cit., De Nardis 2014, p. 230.

4. CONCLUSIÓN Y RECOMENDACIONES

Este documento abordó la gobernanza de Internet desde la relación entre configuraciones tecnológicas y configuraciones de poder. Ese acercamiento crítico busca tomar distancia del enfoque tradicional de las metodologías y las formas. La gobernanza de Internet, antes que el conjunto de instituciones y fórmulas multilaterales de discusión, es un campo de disputa alrededor del control y la gestión de una tecnología.

El estudio de la gobernanza de Internet debe abrirse entonces a todos aquellos que ejercen poder en la red, sin importar el escenario en el que se encuentren. Hacer este esfuerzo requiere identificarlos, entender el tipo de interés que tienen y la forma como influyen en el entorno digital –si administran un recurso crítico o si hacen parte de la infraestructura, por ejemplo–.[66]

Esa visión –sociológica, si se quiere– puede dar luces sobre las motivaciones y expectativas de quienes participan en la gobernanza de Internet, y sobre los puntos de presión y los elementos en disputa. Sin embargo, enfrenta la limitación de no poder responder a la pregunta de cómo debe ser la gobernanza de Internet. Mucho menos puede responder esta pregunta el acercamiento común a este tema, en el cual la gobernanza de Internet es sobre todo la descripción de una serie de procesos.

Esto parece indicar que la gobernanza de Internet no es del todo útil para saber cómo gobernar Internet. Como lo demuestran las fuentes consultadas para este documento, sí resulta útil para describir arreglos institucionales, herramientas de decisión y grupos de interés alrededor de Internet. Pero como marco de referencia para abordar problemas y para proponer soluciones desde la sociedad civil, parece insuficiente.

Para avanzar en una aproximación nueva de la gobernanza de Internet –incluso evitando la etiqueta de ésta como disciplina– es necesario desintegrar el concepto de Internet para, más bien, abordar las tensiones que existen en el entorno digital en diferentes frentes. Una aproximación realista de Internet, plantea Mozorov, debe evitar la reivindicación de valores inherentes –como la transparencia, la apertura– para prestarle particular atención a cómo esos valores se manifiestan en debates específicos. [67]

Buscar un trabajo más táctico no equivale a desconocer que existe una visión hacia donde debe propender una tecnología como Internet. Para De Nardis y Raymond, "*un acercamiento apropiado para una gobernanza de Internet responsable y eficaz requiere determinar qué tipos de administración son óptimas para promover un balance de interoperabilidad, innovación, libertad de expresión y estabilidad operativa en cualquier contexto funcional y político*".[68]

La arquitectura de Internet es el elemento estructurador más relevante a la hora de analizar cómo estos balances se juegan en la práctica. Lo que queda incorporado en el código de la red difícilmente logra deshacerse a través de negociaciones o diálogos posteriores.[69] Así, el seguimiento a las fuerzas que moldean esa infraestructura y la manera como toman las decisiones, debe ser una prioridad para la sociedad civil.

Hasta hoy la sociedad civil –abusando de la generalización– ha promovido la fórmula del diálogo 'multi-stakeholder' como la avenida para enfrentar esos retos. Sin embargo, como se expuso acá, los actores relevantes no llegan a esos escenarios –si es que realmente asisten– con la intención de reevaluar su posición de poder en la red o de aceptar un cambio que consideren adverso a sus intereses. Antes que seguir reprochando esa actitud, hay que entenderla y enfrentarla. Entender esa limitación del modelo 'multi-stakeholder' implica, en otros palabras, "*dejar de verlo como un fin en sí mismo que deba ser aplicado de manera homogénea a todas las funciones de la gobernanza de Internet*".[70]

Ilustremos este punto con el ejemplo del *copyright*. Desde distintos frentes, los agentes interesados en extender la protección del derecho de autor al entorno digital –incluso más allá de lo que originalmente pretendía proteger aquel– vienen promoviendo cambios en todas las capas de la red. Los instrumentos para hacerlo se combinan y retroalimentan: tratados internacionales, leyes, gestión de derechos (D*igital Rights Management*) y asignación de recursos críticos. Sin embargo, las fuerzas no

66 Cfr. Op. Cit. Van Eeten y Mueller.
67 Cfr. Morozov, E. To Save Everything, Click Here: The Folly of Technological Solutionism. PublicAffairs, 2013.
68 Op. Cit., De Nardis y Raymond, 2013, p. 2 (traducción informal).
69 Cfr. Op. Cit. Musiani
70 Op. Cit., De Nardis y Raymond, p. 2 (traducción informal).

están del todo alineadas a su favor: la sociedad civil también promueve protocolos, pero para hacer más fácil el intercambio de contenidos; los Estados tramitan leyes de responsabilidad de intermediarios que no necesariamente siguen la agenda de las industrias creativas, y otras empresas igualmente poderosas se inclinan por entornos digitales menos coercitivos.

En ese contexto, la apuesta por un diálogo 'multi-stakeholder' sin matices no solo es una pérdida de tiempo, sino también una vía que en últimas puede favorecer a quienes esperan tomar todas las decisiones a puerta cerrada. En un escenario tan complejo como el del *copyright*, la sociedad civil debe elevarles a los actores interesados los costos de tomar decisiones a espaldas del interés público; debe buscar los caminos propicios para cuestionar las negociaciones; debe indagar por las modificaciones en el código, y debe litigar los cambios y movilizar a la gente para que los exija. Por supuesto, nada de lo que se acaba de decir es novedoso: muchos grupos ya están inmersos en una tarea similar. El problema, sin embargo, es que montados en la bicicleta estática de los escenarios formales de la gobernanza y el diálogo multisectorial, muchos esfuerzos de coordinación e incidencia se pierden.

Por último, subyace la pregunta sobre el papel del Estado. De un lado, las organizaciones de la sociedad civil les exigen un rol pasivo en el entorno digital. Del otro, esperan una intervención activa en la preservación de los derechos fundamentales y en la supervisión de los intermediarios más poderosos.

Aceptar una visión heterogéneo de la gobernanza de Internet también pasa por asimilar y abrazar esa paradoja: necesitamos exigirle distintos roles al Estado en el entorno digital. Y, de la misma forma, necesitamos que los Estados entiendan que su papel en la gestión y control de Internet varía según el contexto. Mantener un entorno seguro para las transacciones en línea no implica acabar con la privacidad, o asegurarse de que los intermediarios respeten los derechos fundamentales en los servicios que prestan no requiere estatizar la red.

Al final será imposible controlar todos los factores que influyen en el gobierno de Internet. La descentralización de actores y la dispersión del control, en últimas, permiten, por ahora, que nadie tenga todo el poder para llevar este tren en una u otra dirección. Tal vez el rol de la sociedad sea hacer ese ejercicio de equilibrismo.

CELE

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