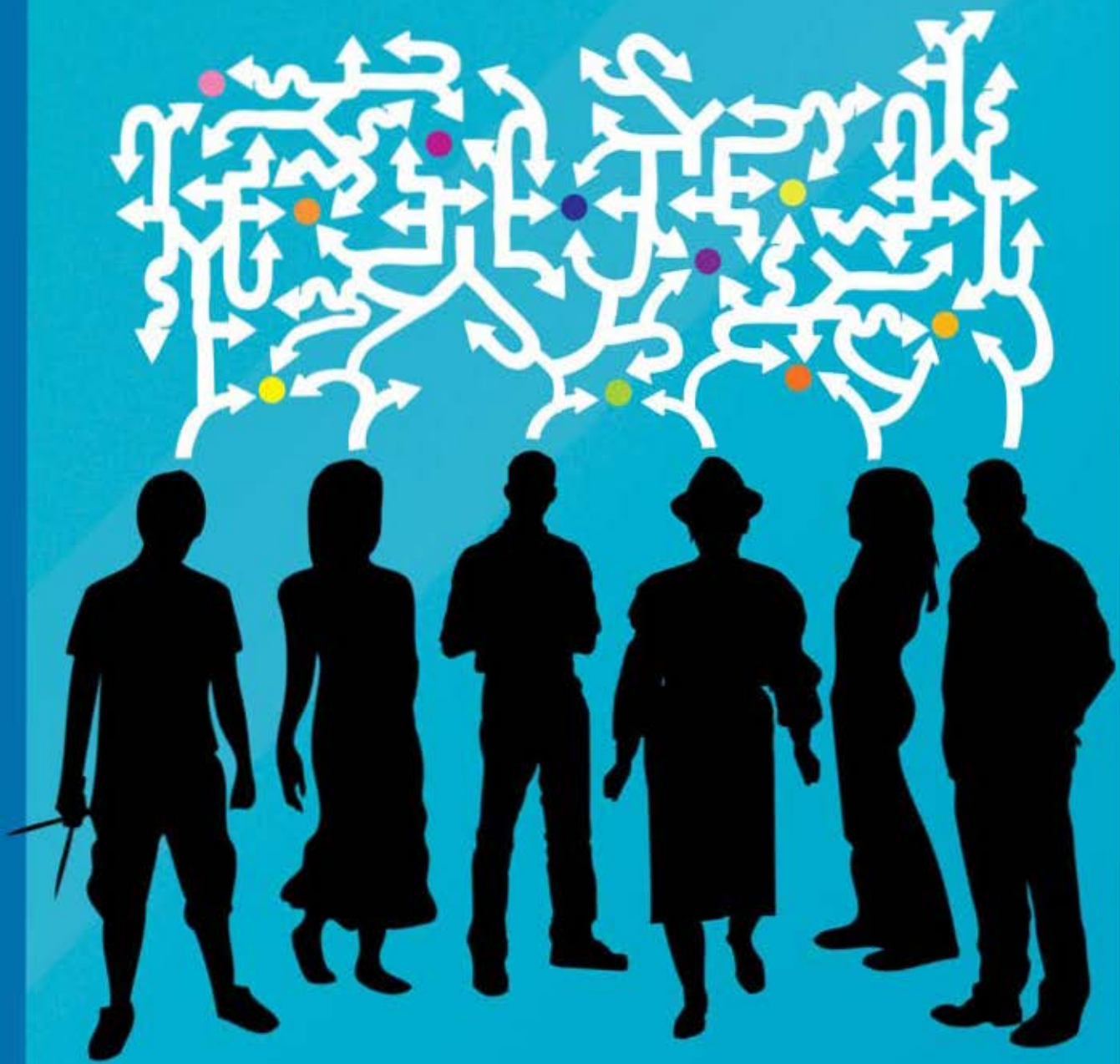
AMERICA LATINA *en movimiento*

503

abril 2015

ISSN 1390-1230

Hacia una Internet ciudadana



www.alainet.org

alai

AMERICA LATINA
en movimiento

Edición digital

503
abril 2015
año 39, 2ª época

Diseño editorial y Portada
Verónica León

Publicación internacional de análisis y opinión de la Agencia Latinoamericana de Información

ISSN No. 1390-1230

Director: Osvaldo León

ALAI: Dirección postal
Casilla 17-12-877, Quito, Ecuador

Sede en Ecuador
Av. 12 de Octubre N18-24 y Patria,
Of. 503, Quito-Ecuador
Telf: (593-2) 2528716 - 2505074
Fax: (593-2) 2505073

URL: http://alainet.org

Redacción:
info@alainet.org

Suscripciones y publicidad:
alaiadmin@alainet.org

ALAI es una agencia informativa, sin fines de lucro, constituída en 1976 en la Provincia de Quebec, Canadá.

Suscripción versión impresa
(10 números anuales)

	Individual	Institucional
Ecuador*	US$ 34	US$ 40
A. Latina	US$ 60	US$ 80
Otros países	US$ 75	US$ 140

* incluye IVA

Cómo suscribirse:
www.alainet.org/revista.phtml
se aceptan pagos por Internet

Hacia una Internet ciudadana

¿Otra Internet es posible?

Sally Burch

Hace apenas 25 años, la gran mayoría de personas no había utilizado nunca una computadora, visto un teléfono móvil ni oído hablar de Internet. Estas tecnologías hoy están tan imbricadas en la vida cotidiana, que nuestras formas de hacer, vivir, trabajar, consumir, relacionarnos, organizarnos, se están transformando velozmente, trayendo muchos beneficios. Internet ya es la principal base de datos mundial para fines educativos, de conocimiento, de trabajo, de consumo y otros; pero por lo mismo, hay cuestiones fundamentales de derechos e interés público, relacionados con el control y poder de decisión. De allí que aparecen nuevos desafíos para el ordenamiento político-económico y la convivencia social, que nuestras sociedades aún no han podido procesar debidamente.

La invasión a la privacidad de las comunicaciones es quizás uno de los ejemplos más evidentes, desde las revelaciones de Edward Snowden sobre el espionaje masivo de la Agencia Nacional de Seguridad (NSA) de EE.UU. Pero hay muchas más áreas donde están surgiendo nuevas problemáticas, entre ellas: la potencial discriminación en sistemas automatizados de preselección de candidatos a empleos, estudios, créditos, y otros; la pérdida de derechos laborales en la nueva "economía del compartir"; o el poder desmedido de una sola empresa privada transnacional –Google– de determinar qué es visible y qué no en la base de datos y conocimientos más grande y más consultada del mundo – o sea, la Web. Ello significa que las decisiones sobre el desarrollo de Internet, sus aplicaciones y usos tienen implicaciones para los derechos humanos, la justicia y equidad social y económica y la democracia, que requieren de un marco de políticas públicas y regulaciones, en lo nacional e internacional.

Sally Burch, periodista de ALAI.

Descentralización o concentración

No cabe duda que Internet, que inicialmente se desarrolló como un sistema relativamente descentralizado, ha permitido el florecimiento de un sinfín de iniciativas de creatividad e innovación. Es, quizás, la primera vez que la población tiene acceso a participar libremente en el desarrollo de una tecnología de punta, en lugar de ser simplemente usuaria. Con su capacidad de adaptación en distintas escalas, esta tecnología ha mostrado su aptitud para potenciar iniciativas ciudadanas o comunitarias, bajo su propio control. También ha contribuido a democratizar el acceso a la información, la comunicación y el conocimiento; y ha permitido la proliferación de espacios –sean abiertos o cerrados– de intercambio libre de ideas, conocimientos, creaciones, donde impera un sentido de bienes comunes y de autogestión.

Bajo conceptos como "los comunes", el software libre y la cultura del conocimiento compartido, se están desarrollando muchas iniciativas de tecnología alternativa, que incluyen redes sociales libres, servicios de mensajería, plataformas de blogs, sistemas de seguridad, incluso un sistema alternativo de nombres de dominio, el Open Root, que es independiente del sistema del ICANN[1].

No obstante, en paralelo ha surgido otra tendencia contraria: hacia la concentración y la centralización. Y es que, debido al llamado "efecto red", donde los usuarios confluyen

1 ICANN: Corporación de Internet para la Asignación de Nombres y Números, entidad que controla este sistema a nivel mundial.

hacia el servicio más exitoso, Internet se ha prestado también a la conformación de grandes monopolios, con una acumulación económica inédita, y con la consiguiente concentración de poder[2]. La "materia prima" de este enriquecimiento es el acumulado de datos (personales y otros) que los usuarios entregan –muchas veces involuntariamente– a estas empresas a cambio de servicios "gratis"; datos que son vendidos a anunciantes, que constituyen la clientela predilecta de estas empresas; mientras que los usuarios, en tanto potenciales consumidores, se vuelven el "producto". Es más, para afianzar el control, los espacios públicos se han ido cercando con "murallas", dentro de las plataformas privadas de las redes sociales digitales, donde las reglas son definidas por la empresa proveedora.

A la par de esta segunda tendencia –y ahora sabemos que con una colusión directa–, se ha universalizado la vigilancia por parte de agencias de seguridad, principalmente de EE.UU. y sus cuatro aliados anglófonos (Reino Unido, Canadá, Australia y Nueva Zelandia – que conforman los llamados 5 Ojos), desconociendo cualquier límite geográfico, legal o ético. Su meta es recabar toda la información posible, de todo el mundo, sobre todos los temas y guardarla indefinidamente. Es sabido que otros gobiernos nacionales también incursionan en mayor o menor medida en tales actividades, dentro o fuera de la legalidad, si bien no en escala tan masiva. Es más, al menos unos 30 países están desarrollando armas cibernéticas, lo que nos podría encaminar hacia una situación de guerras en y a través de Internet, que trae el riesgo de escalar a otros niveles de guerra.[3]

Entre estas dos tendencias contrarias –descentralización, o concentración/ vigilancia/ armas cibernéticas–, la balanza se está inclinando peligrosamente hacia la segunda, con graves consecuencias potenciales para los derechos humanos y la justicia social y económica, e incluso para la misma democracia. Esto ocurre porque las fuerzas del mercado empujan fuertemente hacia la concentración; pero también porque el desarrollo tecnológico de Internet no ha priorizado debidamente la seguridad de los usuarios. A ello se añade que existen pocas medidas en términos de legislación y políticas públicas destinadas a ponerle cierto orden. Incluso hay casos donde la legislación va en sentido contrario, sacrificando la seguridad y privacidad de los usuarios, supuestamente para proteger a la población del terrorismo, aunque sin evidencias de que sea efectivo.

Enfrentamientos legales

Diversas iniciativas recientes están reactivando el debate en torno a los derechos digitales en el mundo. Numerosos gobiernos han adoptado políticas para garantizar la neutralidad de la red. En Brasil y algunos países de la Unión Europea se encuentran legislaciones entre las más avanzadas para los derechos en Internet. Es más, Alemania y Brasil están liderando una iniciativa en la ONU sobre privacidad, luego de las denuncias de Snowden, uno de cuyos resultados es que el Consejo de Derechos Humanos de la ONU nombró hace poco un relator especial sobre privacidad.

Inevitablemente, tarde o temprano, la defensa de los derechos digitales implicará enfrentar el poder desmedido de las grandes empresas transnacionales de Internet. Como nuevo ejemplo de ese poder, este 21 de abril 2015, Google cambió unilateralmente el algoritmo de su buscador para móviles, de manera que las búsquedas ya no tomarán en cuenta los sitios considerados "no amigables" al móvil. O sea, ya no cuenta el contenido, ni la reputación o popularidad del sitio, sino la capacidad de instalar tecnología para móviles, lo que pone en desventaja a muchos sitios de bajos recursos.

Recordemos que más del 60% de las búsquedas en la Web a nivel global (y alrededor de 90%

2 Ver Sally Burch, "¿Cómo desmonopolizar Internet? Entrevista con Robert McChesney", *América Latina en Movimiento*, No. 494 (abril 2014), http://bit.ly/1JlXnAJ

3 Ver el artículo de Prabir Purkayastha en esta edición.

en Europa y América Latina) pasan por Google. La empresa tiene el poder de determinar qué contenidos se privilegian en el horizonte de los internautas y cuáles no se verán nunca. Pero, ¿con qué legitimidad se ha auto-otorgado ese poder? Justamente días antes, la comisionada antimonopolio de la Unión Europea acusó formalmente a Google de abusar de la posición dominante de su buscador, porque sus algoritmos secretos privilegian ciertos contenidos propios sobre otros en los resultados de búsqueda. Google ha anunciado que lo litigará en las cortes y el juicio podría durar años. ¿Cuántos gobiernos tendrán la capacidad de lidiar con gigantes como Google, y aun si lo hacen, qué tanto afectará el poder de las empresas? Recordemos que Google tiene también el gmail, segundo servicio de correo en el mundo; el sistema Android que capta 76% del mercado de smartphones; Youtube, que domina el video online; y es de lejos el mayor vendedor mundial en el enorme mercado de publicidad en línea.

Ahora bien, no son solamente las corporaciones privadas que están en la mira de la defensa de derechos en Internet, sino también ciertos gobiernos y sus agencias de seguridad. Un estudio que acaba de publicar la Comisión Global sobre Gobernanza de Internet, titulado "Hacia un pacto social para la privacidad y la seguridad digital"[4], constata el riesgo actual de la erosión de confianza en Internet y advierte que "Los individuos y las empresas deben ser protegidos tanto del abuso de Internet por terroristas, grupos cibercriminales, como de los excesos por parte de gobiernos y empresas que recolectan y utilizan los datos privados" (p. 9). De conformidad con el derecho a la privacidad reconocido en la Declaración Universal de Derechos Humanos, el estudio afirma que: "el rol de un gobierno debe ser de fortalecer la tecnología de la cual depende Internet y su uso, no debilitarla" (p. 10). El informe insiste en el reconocimiento de la privacidad como derecho humano fundamental; y apela a mayor transparencia y rendición de cuentas de los gobiernos; y proporcionalidad en la vigilancia, conforme a la legislación nacional e internacional de derechos humanos. Demanda también mayor responsabilidad de las empresas que recolectan datos de usuarios, tanto para garantizar la seguridad de los mismos, como para informar y consultar debidamente a los usuarios sobre su uso.

Presidida por el ex primer ministro sueco y líder del partido conservador, Carl Bildt, la Comisión Global sobre Gobernanza de Internet está compuesta por un grupo de alto nivel de 29 personas con influencia en los círculos de políticas de Internet, incluyendo ex altos funcionarios de la seguridad e inteligencia estadounidense y británica. Resulta significativo que un grupo principalmente del *establishment* ya reconozca que se está perdiendo el equilibrio entre los intereses nacionales de seguridad y la privacidad; y que vulnerar la seguridad de los usuarios implica favorecer al crimen e incluso al terrorismo. No obstante, en sus recomendaciones de mecanismos para avanzar, la Comisión defiende el actual modelo "multisectorial" de gobernanza, que en los hechos poco ha respondido a parámetros democráticos.[5]

En los últimos tiempos, también se han tramitado diversas acciones judiciales particulares en las cortes de Europa para comprobar hasta donde los derechos ya reconocidos deben respetarse también en el dominio digital. Y en varias oportunidades, se ha visto un sistema judicial dispuesto a tomar posturas firmes en defensa de los derechos humanos frente a gobiernos y corporaciones privadas, y así sentar precedentes. Tales casos incluyen un juicio en la Corte de Justicia Europea contra Facebook por la seguridad y trato de los datos de usuarios europeos, en vista de su colaboración con agencias de inteligencia en programas como Prism. La misma Corte también respaldó el "derecho a ser olvidado" (o sea, a solicitar la eliminación de datos personales de los busca-

4 *Toward a Social Compact for Digital Privacy and Security*, Statement by the Global Commission on Internet Governance, http://bit.ly/1DZWeKP

5 Ver el artículo de Norbert Bollow en esta edición.

dores). En otro caso, un tribunal de Reino Unido reconoció el derecho de usuarios del navegador Safari de Apple a reclamar a Google por haber retenido y vendido sin su autorización datos sobre sus hábitos privados de navegación[6].

Por su parte, en 2014, la misma Corte Europea invalidó parcialmente la Directiva de Retención de Datos de la UE, de 2006, al considerar que obligar a los proveedores de comunicación a retener todos los metadatos (o sea, quien comunica con quien) interfiere indebidamente con los derechos fundamentales de privacidad.

En cuanto a los países del Sur, pocos tendrían la capacidad de enfrentar a las corporaciones de Internet en las cortes. De hecho, más bien algunos les están abriendo aún más las puertas, acogiendo por ejemplo la iniciativa Internet.org de Facebook, que supuestamente extiende el acceso de sectores pobres a Internet desde su móvil, pero que en la práctica equivale a una "Internet pobre para pobres" que de entrada les ata a las plataformas corporativas, y esto, en flagrante violación del principio de neutralidad de la red. Hasta ahora, en América Latina, solo Chile se ha parado en firme para rechazar el ingreso de Internet.org [7]. Por supuesto, es valioso pensar en alternativas para que las comunidades empobrecidas pueden acceder a la tecnología, pero hay otras opciones posibles que no implican la dependencia de los espacios corporativos, como por ejemplo la iniciativa guifi.net de Cataluña, que ha sido premiada por interconectar comunidades con equipos autogestionados a muy bajo costo.

Hacia un Foro Social de Internet

Está creciendo el entendimiento de que difícilmente se podrá comenzar a alterar las tendencias actuales en la configuración de poder y el sistema de gobernanza de Internet, si no se construye un amplio movimiento social de presión con este fin. Como contribución a este propósito, a inicios de 2015, diversas organizaciones lanzaron la idea de organizar un Foro Social de Internet (FSI), con el carácter de un foro temático vinculado al proceso del Foro Social Mundial (FSM). Más de 80 organizaciones[8] se han sumado al llamamiento inicial y la iniciativa fue debatida en el FSM en Túnez, en este mes de marzo.

El FSI[9] se presenta como un espacio para debatir sobre "la Internet que queremos y cómo construirla antes de que la revolución del conocimiento y del acceso a la información sea secuestrada irremediablemente por los intereses corporativos y las agencias de seguridad, incrementando el nexo de corrupción entre la política y el dinero".[10]

La intención es sumar a una amplia gama de organizaciones, movimientos sociales y luchadores y luchadoras sociales que comparten este objetivo, ya que Internet se ha convertido en una herramienta y espacio de intercambio y consulta indispensable para el trabajo organizativo y las causas sociales. Con ellas se propone crear un mecanismo democrático de organización del FSI, que, entre otros aspectos, definirá las modalidades, el lugar y la fecha del Foro.

¿Por qué el formato de un Foro Social? La convocatoria expone que el Foro Social de Internet (FSI) está inspirado en los procesos del Foro Social Mundial (FSM) y su visionaria convocatoria de que "Otro mundo es posible", adoptando el lema de que "Otro Internet de los pueblos es posible". Recordando la Carta de Principios del FSM, que apela a un proceso de globalización diferente al "comandado por las grandes corporaciones multinacionales

6 Sobre los casos mencionados ver: Julia Powles, *Data privacy: the tide is turning in Europe - but is it too little, too late?*, http://bit.ly/1c0EOUQ

7 Al respecto ver el artículo de Parminder Jeet Singh en esta edición; y también: María del Pilar Sáenz, *Hacia tierras más libres en Internet*, http://bit.ly/1G17pTZ

8 http://bit.ly/1DHVKFK

9 http://bit.ly/1Gg25Kj

10 *Llamamiento Túnez para la Internet de la ciudadanía*, http://bit.ly/1DHVMNP

y por los gobiernos e instituciones que sirven a sus intereses", el FSI apuesta "a un Internet desde abajo, controlado por el pueblo, incluyendo a quienes aún no están conectados"[11].

En las siguientes páginas de esta revista, personas vinculadas a este proceso exploran algunos de los temas relevantes para construir una Internet de los pueblos, o una Internet ciudadana, más justa, equitativa y democrática.

11 *Llamado al Foro Social de Internet*, http://bit.ly/1DsjChm

La importancia de la maleabilidad de la propiedad intelectual

Tan abierto, tan cerrado

Pedro Cagigal

Muchas palabras se han ido incorporando al discurso de activistas y políticos desde la popularización de los medios digitales: libre, abierto, compartir, transparencia, red y demás. Si bien parte del léxico parece afín a la izquierda y ha sido promovido como tal, en realidad estos términos transitan indiscriminadamente en los más variados discursos políticos.

En lo que parece ser un giro del capitalismo, vemos como compañías basadas en lo digital empiezan a ganar terreno a las usuales corporaciones predominantes de banca, minería y petróleo. En diciembre 2014, Apple reportó el mayor ingreso trimestral generado por una corporación en la historia. En 2013, WhatsApp, una compañía con cerca de 50 empleados y una infraestructura pequeña, fue adquirida por Facebook por 19 mil millones de dólares (12 de los cuales fueron pagados con acciones). Mark Zuckerberg (co-fundador de Facebook) pagó no solo por el nombre y la red establecida, sino también por la información de sus 400 millones de usuarios, o mejor dicho, por esos usuarios; y así, por la eliminación de la competencia. Hay muchos ejemplos de este tipo de adquisiciones y fusiones, muchas *startups* están diseñadas para ser compradas por grandes corporaciones. Esta nueva cara del capitalismo revela la tendencia hacia la estructuración en monopolios de la economía digital y cognitiva. Recordemos que cuando hablamos de propiedad intelectual, hablamos de monopolios legales sobre conocimientos, saberes y productos culturales.

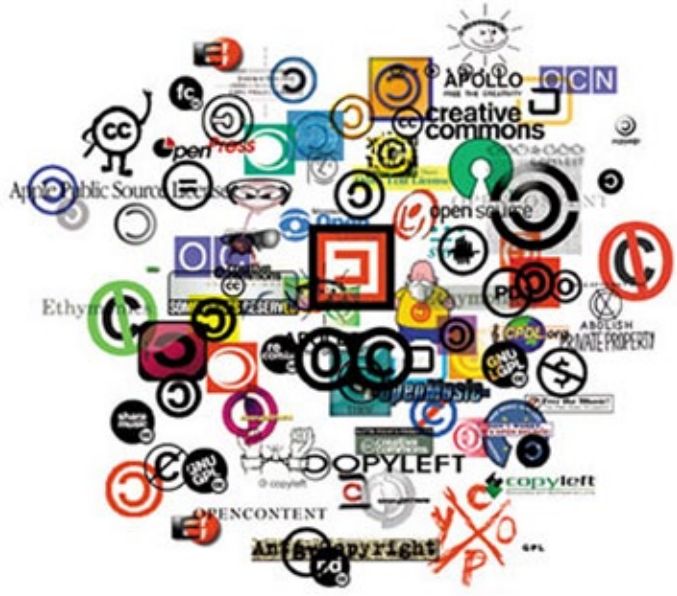
En la bolsa, las compañías dependen de la valoración abstracta y especulativa de su *marca* –propiedad intelectual–. Esta valoración está atada a la infraestructura y reputación de la empresa (tamaño, eficiencia, mercado y capital simbólico), pero también tiene que ver con la 'posesión' y monopolio de conocimientos e información. El acaparamiento, clasificación y nuevos sistemas de análisis de datos masivos son la tendencia, así mismo, la acumulación de patentes. La economía digital se ha estructurado en base a la transacción comercial de la información e innovación generada, recopilada y apropiada. Mucho de este comercio se hace bajo las normas de propiedad intelectual internacional: patentes, marcas y copyright. Sin embargo, la información que producimos al navegar, e incluso parte de lo que voluntariamente dejamos en diversas aplicaciones en la red, no está sujeta a reclamo de autoría, sino a los términos y condiciones de cada sistema. En resumen: si usas esta tecnología, aceptas obligatoriamente todas las condiciones impuestas (incluso a entregar tu alma inmortal, como una aplicación de videojuegos británica irónicamente incluyó en sus términos de uso).

Términos en disputa

En el sistema de propiedad intelectual global ha existido una tendencia histórica a proteger más y por más tiempo a los poseedores de los

Pedro Cagigal actualmente es investigador de procesos de ciencia y tecnología en América Latina para FEDAEPS, Quito. Posee una maestría en Cultura y Sociedad Digital.

derechos de comercialización –no necesariamente los autores–. Sin embargo, los derechos sobre los contenidos y datos creados por los usuarios en la red han sido completamente descartados de las normativas autorales. Europa ha establecido algunas regulaciones iniciales sobre la información en red. Por ejemplo, se establece la necesidad de autorización sobre la venta de datos a terceros, sin embargo la opción sigue incluida en los términos que debes aceptar para acceder. También se ha establecido el derecho a ser olvidado, algo polémico, pues quienes más lo solicitan son personas con antecedentes penales. Si bien el derecho a rehacer su vida es legítimo, hay sectores que consideran que ciertos delitos graves o de alta corrupción no deberían ser olvidados. Por supuesto, para quienes pueden pagárselo, hay empresas que se dedican a borrar "huellas digitales", más allá de las normativas.



Después de las revelaciones de Edward Snowden sobre la vigilancia masiva de la NSA y la GCHQ (agencia de seguridad de Inglaterra), la privacidad y la seguridad se han convertido en los principales términos en la opinión pública para abordar la noción de derechos digitales. La economía cognitiva pregunta: ¿está dispuesto a pagar por los servicios que antes eran gratuitos si le ofrecemos mejor seguridad? Así, los derechos digitales, antes de ser plenamente establecidos, comienzan a ser entendidos como mercancía. Pero más allá de los importantes derechos a la intimidad, confidencialidad de datos y honra pública, también podríamos cuestionarnos si tenemos derecho a decidir sobre la comercialización de nuestros datos a terceros fuera de la lógica del todo o nada. En caso de venta, ¿tenemos un derecho de beneficio? En la lógica de las aplicaciones 'gratuitas', el servicio se da a cambio de nuestra información, ese es el acuerdo. Pero examinando el poder y el tamaño que están adquiriendo unas pocas empresas en Internet, y el enorme potencial de esa información, podríamos cuestionarnos como sociedad y como Estados si este es un intercambio justo.

En 1950, el antropólogo Marcel Mauss planteó, a partir del estudio de economías ancestrales, su noción de *Economía del Don*. Dar o aceptar un regalo, más allá de un acto solidario, constituía un ejercicio de poder e interés, que de alguna manera ataba a quién daba y a quien recibía. Desde la teoría marxista, Tristana Terranova parte de esta noción y nos habla de 'labor gratuita', una nueva forma de explotación laboral en lo digital, en que toda nuestra interacción es comercializable, incluso, el trabajo voluntario por el bien común acaba beneficiando directa e indirectamente a las grandes compañías. Muchas de éstas colaboran con el desarrollo de software libre y abierto a través de financiamiento y talento humano, usualmente ofreciendo flexibilidad laboral a sus programadores. Si Linux-Ubuntu es uno de los sistemas operativos más usados del planeta es porque Google, y su importante porcentaje de computadoras, corre bajo Goobuntu, su versión adaptada.

Se vuelve complicado oponer ideológicamente lo libre, lo abierto y lo privativo, y demarcar una derecha e izquierda claras. Los términos

digitales se vuelven términos en disputa. Sin duda, el *software libre* ha detonado nuevas dinámicas de organización productiva, nuevos sistemas de negocio, ha promovido actitudes autodidactas y generado comunidades políticas, incluso partidos como el *Pirate Party*. Pero el *libre* también está cargado de una ideología liberal de desregularización. Por su parte, el *software abierto*, manteniendo la idea de código accesible, adoptó una actitud más pragmática y flexible hacia el mercado. Para Nathaniel Tkacz[1] el *abierto* se basa en los mismos valores que las democracias neoliberales: libertad, individualismo, competencia e intercambio. Lo abierto oculta sus cierres; como colaborador en software puedes acceder al código solo si tienes los conocimientos y herramientas, puedes escoger entre ciertas tareas, no puedes cambiar la estructura de distribución de labores, ni menos la de negocios. Con lo *transparente*, sucede igual: puede ser sinónimo de honestidad, pero también tiene la connotación de la vigilancia permanente y su subsecuente disciplinamiento interno a través de la mirada de otros. La misma noción de la economía del compartir (*sharing economy*) se ha convertido en el capital simbólico de un puñado de empresas –millonarias– de Silicon Valley, como *Uber*.

Formas de propiedad

Los medios digitales son muy seductores, nos ofrecen juegos, información, nos han dado la plasticidad y comodidad para construir identidades virtuales y nuevas formas de relacionarnos y comunicarnos. Nuestra participación sostiene su economía, por eso nos repiten: cuéntenos su vida, háganos saber si le gusta esto o aquello, tomémonos juntos su tiempo al correr, genere redes, invite amigos. En esta saturación, bien podemos recordar el valor de decir nada que Deleuze plantea: las fuerzas represivas no pretenden detener que nos expresemos, más bien, nos obligan a expresarnos constantemente.

Suena un tanto desalentador que todo el potencial de participación social a través de la red acabe revitalizando al capitalismo; sin embargo, no hay que desmerecer lo que estos mecanismos han generado: nuevas formas de organización social a través del trabajo solidario, el conocimiento y los intereses compartidos, creando comunidades no determinadas por geografía y no condicionadas a intereses comerciales. También se puede decir, como Martín Petersen[2] argumenta, que el gran aporte del software libre es la posibilidad de pensar en distintas formas de propiedad: el copyleft establece un tipo de propiedad que se mantiene en el dominio público, las licencias Creative Commons (CC) dan diversas opciones para la difusión creativa sin truncar su capacidad de comercialización. Pero además de estos ejemplos, podemos pensar que la propiedad intelectual puede ser definida de muchas otras maneras a través de licenciamientos nuevos. Y ahí el CC y copyleft se quedan cortos en poder generar también licenciamientos comunitarios, asociativos, nacionales o regionales, con enfoques en los saberes de las comunidades ancestrales, o específicos para la música o el cine. La forma en que definimos nuestras propiedades creativas influencia directamente nuestros modelos de negocios y asociaciones de trabajo, como lo ha demostrado el software.

Pensar en nuevos licenciamientos, nuevas propiedades menos monopólicas, no solo nos genera alternativas al actual sistema global de propiedad intelectual –pilar del neoliberalismo–, sino que también puede plantear cambios al Estado. La defensa de la propiedad privada ha definido el rol del Estado capitalista; alterar el sentido de propiedad, esta propiedad 'inmaterial' motor de la nueva economía, y hacer que el Estado reconozca responsabilidades sobre otras posibles propiedades –públicas, comunitarias, asociativas– es un medio para alterar la lógica misma del Estado.

1 Tkacz, N. (2012). From open source to open government: A critique of open politics. *Ephemera*, *12*(4), 386.

2 Pedersen, M. (2010). Free culture in context: Property and the politics of free software. *The commoner*, (14), 40-136.

Seguridad versus privacidad, derecho a la resistencia

Montserrat Boix

Podría parecer demasiado simple iniciar una reflexión sobre privacidad, seguridad y libertades en Internet con la referencia a los ataques contra las Torres Gemelas de Nueva York el 11 de septiembre de 2001. Expertos en inteligencia y terrorismo reconocen que el 11S fue "un día más" de un proceso que se venía gestando muchos años antes[1]; pero la fecha marca sin duda un punto de inflexión en lo que se ha convertido en recurrente durante esta última década: la utilización por parte de algunos gobiernos de acontecimientos violentos y traumáticos para justificar el recorte de libertades y provocar un estado colectivo de miedo, con el objetivo de que la ciudadanía acabe cediendo su privacidad, algo que sería inadmisible en otros momentos, con la promesa de mayor seguridad.

En poco más de una década, EEUU, utilizando enemigos mundiales más o menos reales y el argumento de combatir el terrorismo global, ha logrado trasladar a todo el planeta el mensaje de que la solución en este mundo cada vez más inseguro está en el control masivo. De poco ha servido que se haya demostrado ya que se trata de un falso dilema, que una mayor vigilancia de la población no implica la reducción de amenazas terroristas y que, sin embargo, puede tener efectos altamente perversos.

Ser investigados sólo por utilizar Internet conculca derechos básicos. El anonimato es vital para una sociedad abierta y libre[2]. Tenemos derecho a comunicarnos libremente por Internet sin ser vigilados.

Informarnos, reflexionar con serenidad, posicionarnos, establecer los límites que nos permitan salvaguardar los derechos individuales y colectivos y exigir a gobiernos y corporaciones su respeto marcará el futuro de nuestras sociedades y la propia supervivencia de la democracia.

"O estás con nosotros o estás con los terroristas"

El 20 de septiembre de 2001 en un discurso ante el Congreso de EEUU, dirigido también a la nación, el entonces presidente George W. Bush develaba el diseño del nuevo escenario: el terrorismo era "*una amenaza continua*" y la nueva estrategia defensiva afectaría a todos los ámbitos con un marco global, "*con operaciones visibles y otras encubiertas y secretas*", "*nos uniremos* –avanzaba el dis-

1 José María Blanco. Seguridad e Inteligencia después del 11-S http://bit.ly/1HA92Ke

2 Electronic Frontier Foundation. Anonimato y cifrado http://bit.ly/1IQAC4B

Montserrat Boix, periodista catalana, creadora de "Mujeres en Red", red feminista en Internet. Investigadora en ciberfeminismo y hacktivismo. Profesora de TIC y sociedad civil en diversos masters universitarios en España. Activista en el movimiento de Software Libre y Cultura Libre.

curso– *para fortalecer nuestras capacidades de inteligencia, para conocer los planes de los terroristas antes de que actúen y encontrarlos antes de que ataquen*" y una advertencia que ha logrado calar profundamente y marcar una lógica binaria de la que ha resultado difícil escapar: "*o estás con nosotros o estás con los terroristas*"[3].

La consecuencia directa fue el florecimiento de la industria privada de la inteligencia, la creación de productos destinados al espionaje y la interceptación masiva de comunicaciones[4], y el desarrollo de un sistema de vigilancia mundial sin restricciones. Autoridades legales secretas facultaron a la NSA (Agencia de Seguridad Nacional de EEUU) para revisar los registros telefónicos, de Internet y la localización de grandes grupos humanos. Un proceso que permaneció en secreto hasta las revelaciones de WikiLeaks.

A partir de 2010 la mayor filtración de documentos secretos de la historia, con más de 250.000 cables o comunicaciones entre el Departamento de Estado de Estados Unidos y sus embajadas[5] y la de correos electrónicos fechados de 2001 a 2011 de la agencia de inteligencia privada Stratfor[6], revelaron la cara oculta de un sistema poco o nada respetuoso con los Derechos Humanos y la legalidad, dedicado a espiar a políticos, periodistas, disidentes y activistas, con la complicidad por su silencio de los grandes medios de comunicación.

En junio de 2013, las sospechas se convierten en certezas con las revelaciones de Edward Snowden, excontratista de la CIA y la NSA. Aportan pruebas de la existencia de una red de colaboración entre decenas de agencias de inteligencia de varios países para expandir y consolidar la vigilancia globalizada. Sus documentos nos permitieron conocer la utilización por la NSA de programas como PRISM, que desde 2007 facilitaba el espionaje a 35 líderes mundiales a través de sus teléfonos móviles[7] y daba acceso directo a los datos de Google, Facebook, Apple y otros gigantes de Internet[8], o Xkeyscore, un programa capaz de detectar la nacionalidad de los extranjeros mediante el análisis del lenguaje en correos electrónicos interceptados, aplicado en América Latina, especialmente en países como Brasil, Colombia, Ecuador, México o Venezuela[9]. Las aportaciones de Snowden confirman también que se ha logrado romper la criptografía del sistema financiero mundial.

"*Se ha abierto una brecha entre lo que la gente del mundo cree han sido sus derechos y lo que sus gobiernos han regalado a cambio de información útil sólo para el propio gobierno*" denuncia el profesor Eben Moglen[10] en su artículo "*Privacidad bajo ataque; los archivos de la NSA revelaron nuevas amenazas a la democracia*". La empresa privada ha sacado provecho de la confusión y el shock que nos ha producido descubrir la utilización impune de nuestros datos; y los gobiernos se están beneficiando también de ello, poniendo en peligro la supervivencia de la propia democracia. La nueva situación nos interpela de manera individual y colectiva: la privacidad está relacionada con nuestro entorno social, no se trata de transacciones aisladas que individualmente hacemos con los demás. Cuando regalamos nuestra información personal también estamos socavando la privacidad de otras personas. La privacidad, señala Moglen, es siempre una relación entre muchas personas, no una transacción entre dos.

3 http://1.usa.gov/1fydk3b

4 Así se mueve el negocio del espionaje masivo de las telecomunicaciones. Wikileaks publica la tercera entrega de los Spyfiles. http://bit.ly/1Pvc98S

5 http://bit.ly/1Dk8mCu

6 http://bit.ly/1z1eZi2

7 http://bit.ly/1tGs7Em

8 Glenn Greenwald and Ewen MacAskikll. NSA Prism program taps in to user data of Apple, Google and Others. http://bit.ly/193WyKq

9 Glenn Greenwald, Roberto Kaz e José Casado. Espionagem dos EUA se espalhou pela América Latina http://glo.bo/1GpoXcH

10 Eben Moglen (EEUU 1959) es profesor en la Universidad de Columbia, director de la Software Freedom Law Center y colaborador de la Fundación del Software Libre.

El mundo está polarizado entre quienes consideran que nadie puede impedir el control y quienes se preguntan por qué debería importarnos este control si no estamos haciendo nada malo. Y la respuesta que nos debemos a nosotros mismos -concluye- debe ser: *si no estamos haciendo nada malo entonces tenemos derecho a la resistencia*[11]

Autonomía y soberanía tecnológica

Mientras el poder trata de controlar o influir en los flujos de información en la red con el fin de consolidar su propia posición de poder, millones de personas están implicadas en crear espacios abiertos, transparentes y libres defendiendo el valor de lo público.

Se trata de recomponer la red desde los intereses de "lo común" con tecnologías que permitan a quien las use liberarse de su dependencia con los proveedores comerciales y del seguimiento policial generalizado. Servidores autónomos, redes descentralizadas, enlace entre pares, compartir saberes, lugares de encuentro y trabajo cooperativo[12].

Recuperar el valor de la privacidad:

a) reclamando el secreto del contenido que comunicamos y el anonimato de quien envía y recibe los mensajes, o durante nuestras búsquedas en Internet. Para garantizarla es imprescindible la encriptación tanto en el momento de la transmisión cómo en el almacenamiento de datos locales. Y

b) tomando conciencia del valor de nuestra identidad electrónica y su impacto en nuestras vidas cotidianas evitando delegarlas a las multinacionales. Cuando estamos utilizando Facebook o Google estamos trabajando gratuitamente para los servicios de inteligencia, denuncia Julian Assange, fundador de WikiLeaks. *"Las personas simplemente están haciendo miles de millones de trabajo gratuito para la CIA, al poner en la red a todos sus amigos, sus relaciones con ellos, relatando lo que están haciendo"*. La tecnología está siendo desarrollada en favor de la vigilancia en masa y la información vendida[13].

"En el terreno alimentario los grupos de autoconsumo se autoorganizan para tener sus proveedores directamente, ¿entonces por qué la gente no se autoorganiza con sus proveedoras tecnológicas, comprando directamente el soporte tecnológico que necesita en su vida, igual que las zanahorias?" señala Alex Haché desarrollando el concepto de Soberanía tecnológica[14].

Imprescindibles hardware y software libres, para permitir que cualquiera pueda examinar el código fuente abierto.

Y la descentralización de infraestructuras físicas para hacerlas menos vulnerables a la vigilancia. También su ubicación. El que casi todas las conexiones de Internet pasen por cables de fibra óptica que atraviesan EEUU ha facilitado el robo masivo de información. Se imponen las alianzas industriales para crear la infraestructura física alternativa e iniciativas como la de Brasil que ha anunciado ya el despliegue de su propio cable entre Fortaleza y Lisboa. La instalación que se espera termine en 2016 tiene como objetivo evitar que los datos queden expuestos a pinchazos en territorio de Estados Unidos[15].

Se impone la creación de un marco jurídico que sea vinculante para los estados y establezca Internet como un campo inviolable. La ciudadanía tiene que exigirlo, porque tiene derecho a estar protegida.

11 Privacy under attack; the NSA files revealed new threats to democracy. http://bit.ly/1opgqjr

12 Alex Haché. Soberanía tecnológica.

13 Julian Assange: Facebook y Google son un increíble instrumento de control masivo http://bit.ly/1Gpp5Jd

14 Alex Haché. Soberanía tecnológica.

15 Brasil desplegará su propio cable submarino de Internet para evitar "pinchazos" de la NSA http://bit.ly/1CzeJlq

Desafíos técnicos y políticos para una Internet más segura

ALAI

Si miramos hacia nuestro futuro digital, se puede decir que nos encontramos en la "etapa infantil". A medida que nuestras actividades incorporan un componente digital, la división entre los dominios físico y virtual se vuelve cada vez más indistinguible. De cómo se maneje ese futuro digital, con qué criterios y prioridades se desarrolle la tecnología y qué políticas públicas se implementen, dependerá en gran medida el perfil de ese futuro y sus implicaciones para la seguridad, los derechos humanos, la democracia y la justicia social.

Nuestra «infancia digital» en muchos aspectos se presenta prometedora y ciertamente tiene muchos encantos; pero también van apareciendo nuevas amenazas: inseguridad, vigilancia generalizada, pérdida de privacidad, concentración de la riqueza, control centralizado y poder de manipulación... y la lista se sigue alargando.

Por lo mismo, la expansión ubicua de estas tecnologías significa que estas cuestiones se están tornando demasiado importantes como para dejar únicamente a los especialistas decidir sobre las soluciones, ya sea a nivel técnico o político.

Sin embargo, para la gran mayoría de la ciudadanía, el tratar de entender lo que podemos hacer para mejorar nuestra propia seguridad y privacidad, o incluso para influir en cómo se desarrolla este nuevo mundo digitalizado, parece un reto bastante desalentador. Las revelaciones de Edward Snowden han minado la confianza en los gigantes de la tecnología y en la fiabilidad y seguridad de los software, hardware, aplicaciones y servicios que prestan; pero también nos hacen sentir más impotentes para saber qué hacer para que cambie de rumbo, o incluso cómo salir del sistema.

Dos de las tendencias técnicas más preocupantes en la actualidad son la inseguridad tecnológica y la llamada «Internet de las cosas», según el investigador sueco ***Ola Bini***, de la empresa de software ThoughtWorks. ALAI dialogó con este especialista en seguridad, privacidad y anonimato, respecto a estos desafíos.

"Internet está construida sobre cimientos muy inseguros", afirma. "Por ejemplo, para conectarnos a bancos y otros sitios web seguros, estamos utilizando formas de comunicación que en realidad no son tan seguras como deberían ser". Los ataques de alto perfil, como robo de números de tarjetas de crédito, están en crecimiento.

Un segundo gran problema viene con la proliferación de dispositivos conectados: lo que hoy se conoce como "Internet de las cosas"; por ejemplo, las "casas inteligentes", donde los dispositivos tales como los controles para alarmas de fuego, calefacción y luces están conectadas a Internet y entre sí, lo que permite el acceso remoto. "Suena fantástico hasta que te des cuenta que actualmente estas cosas se construyen sin ningún tipo de seguridad," advierte Bini. Cita recientes ejemplos de un error en la actualización de un sistema que dejó a numerosas casas sin calefacción ni iluminación; o de un hotel de lujo en China que proveyó

iPads a todos los huéspedes para controlar los parámetros de su habitación, hasta que se descubrió que les permitiría controlar cualquier habitación del hotel.

«Pero lo que más me asusta en realidad son los autos», comenta Bini, «porque ahora son computadoras sobre ruedas. Un auto típico tiene más de mil mini-ordenadores incorporados, que significa más de 500 millones de líneas de código. En la industria del software, sabemos que en una base de código de 500 millones de líneas, se puede esperar alrededor de 5 millones de defectos. Esa es una cifra conservadora». La mayoría de ellos pueden no ser tan problemáticos, pero incluso 10 defectos que podrían hacer que el auto se accidente resulta realmente aterrador, y aún más -añade- cuando personas ajenas podrían acceder a ellos para atacar a su auto.

Centralización y balcanización

Desde el punto de vista político, el investigador de seguridad se preocupa por la fuerte tendencia hacia la centralización, pero también hacia la "balcanización" de Internet. "Ambas tendencias refuerzan las estructuras económicas existentes, lo que significa que EE.UU. tienen un poder excesivo sobre lo que sucede en Internet actualmente. Y a pesar de que Internet está construida de tal manera que podría ser descentralizada en todo el planeta, en realidad eso por ahora no ocurre; Internet es centralizada, y EE.UU. tiene el poder sobre básicamente todo lo que sucede».

En cuanto a la balcanización, Ola Bini señala dos aspectos. «La primera de ellas es que está sucediendo como una respuesta a la centralización por parte de EE.UU. y a las revelaciones de Snowden; así, algunos países como Brasil y Rusia se encuentran tramitando legislaciones que obligan a que los centros de datos se ubiquen físicamente en el país del usuario cuyos datos se almacenan». Esto significaría que una empresa como Facebook tendría que almacenar información sobre usuarios rusos en un servidor en Rusia. Facebook quizás podría tener los recursos necesarios para crear sus propios centros de datos, incluso en un gran número de países; pero si más países adoptan una legislación similar, para una empresa que inicia, le resultaría muy difícil crear aplicaciones que se puedan utilizar en más de un país. «Así que el problema es que no es escalable, lo que de hecho podría intensificar la centralización», expresa. Y da un ejemplo más extremo: «Brasil ha estado hablando de la creación de su propia Internet completamente independiente, donde la mayoría de servicios que se utilizan hoy sean servicios brasileños. Pero desde la perspectiva puramente económica, sería muy difícil duplicar todos los servicios existentes en Internet», por lo que podría crear una situación de desventaja para la población brasileña.

El investigador de seguridad considera que Internet debe idealmente permitir a la gente en todo el mundo estar conectada y proveerse servicios entre sí, independientemente de donde se encuentren; y poder hacerlo de forma descentralizada, sin que ningún país pueda interferir en ello. Sin embargo, las actuales tendencias hacia la centralización y la balcanización van en un sentido exactamente opuesto.

Ante esta situación, le preguntamos a Bini qué tipo de innovaciones o políticas podrían ayudarnos a avanzar hacia una Internet más descentralizada. «Hay un montón de cosas que se podría hacer» –respondió–. «Un ejemplo es la neutralidad de la red, que es una solución a corto plazo. En el largo plazo, necesitamos soluciones técnicas que realmente hagan irrelevante la neutralidad de la red. Pero en el corto plazo tenemos que asegurarnos de que una empresa no pueda comprar un servicio preferencial». Tanto en EE.UU. como en varios países de América Latina se están introduciendo medidas sobre la neutralidad de la red, para obligar a los proveedores de servicios de Internet (PSI) a tratar todo el tráfico en Internet por igual, sin carriles rápidos para quienes pagan por ellos.

Una cuestión diferente es la legislación en torno a la conservación de datos, que tiene más que ver con la vigilancia. La mayoría de los países están obligando a los PSI a retener los

datos entre 6 y 24 meses (estamos hablando de los metadatos: quien habla con quien). Esto resulta caro para el PSI, lo que perjudica a los proveedores más pequeños; es más, se les podría exigir que entreguen datos a los servicios de inteligencia. «A diferencia de la neutralidad de la red, la disputa en torno a la conservación de datos está yendo por el camino equivocado», comenta Bini.

En el plano de las aplicaciones, considera que la innovación más importante sería una mayor descentralización de los servicios. «Tenemos que fomentar, por ejemplo, alternativas a Facebook, que estén realmente diseminadas por todo el planeta y donde los datos se almacenen cerca del usuario en lugar de estar cerca de Facebook». En el plano físico, los mapas de conectividad de cables submarinos y de flujos de tráfico demuestran cómo la topología está muy centrada en torno a Estados Unidos, lo que también hace que sea más barato enrutar el tráfico a través de EE.UU. Contrariamente a lo que cabría esperar, mucho tráfico nacional en América Latina se enruta a través de Miami para regresar al país. Se requiere, entonces, cambiar la infraestructura física: «necesitamos tener cables de mayor capacidad que conecten otros países, entre los países del Sur global, para que podamos enrutar el tráfico sin tener que pasar por el Norte global".

Comentamos a nuestro interlocutor que uno de los obstáculos para la descentralización es el llamado efecto de red, según el cual una mayoría de usuarios fluye hacia el servicio más exitoso, lo que contribuye a una centralización aún mayor. El investigador reconoce que eso es algo muy difícil de contrarrestar. «Significa que uso Skype porque mis padres usan Skype y utilizo Facebook porque todos mis amigos en Suecia utilizan Facebook». Sin embargo, considera que es posible crear aplicaciones que funcionan de una forma similar a Facebook, pero «sin tener todos los datos almacenados en servidores de Facebook». Podría tener una funcionalidad similar, salvo que los datos personales se almacenarían cerca del usuario, bajo su propio control, quizás incluso en sus propios aparatos. El usuario decidiría qué datos quiere compartir, por ejemplo con Facebook, para que sean accesibles a sus amigos. Facebook podría hacer correr sus algoritmos sobre esos datos, pero lo más importante es que no serían propiedad de la empresa.

El problema, de acuerdo con Bini, es que, si bien ya es posible construir tales sistemas descentralizados, «no existe el incentivo económico para hacerlo, y en gran parte eso se debe a que Internet actualmente está motorizada por la publicidad». Él anhela que, en unas pocas décadas, viendo este pasado de Internet, la gente lo catalogará como la época oscura, porque «cuando una empresa es financiada con publicidad, significa que no eres el usuario, eres el producto». Así, para Google o Facebook, el incentivo real para proporcionar un buen servicio no es al usuario, sino a los anunciantes en la red. «Mientras esto siga sucediendo, será muy difícil desplazar estos modelos centralizados, porque se basan en la idea de que, para vender más anuncios mejor adaptados a tu perfil, tendrán que utilizar cada vez más tu información personal para lograrlo». Así, dice, las alternativas son que, quizás tendremos que volver a pagar por los servicios, o podríamos ir hacia un modelo donde el gobierno intervenga y ofrezca este tipo de plataformas como servicios públicos.

Soluciones tecnológicas y políticas

Uno de los debates en curso en la comunidad técnica es sobre cuáles problemas pueden o no ser resueltos a través de la arquitectura técnica, y cuáles pueden o no ser manejados mejor mediante políticas públicas. Bini concuerda que es complejo. "Muchos de estos temas, especialmente cuando se trata de la vigilancia y la topografía de Internet –siendo ambas relacionadas–, deben resolverse desde la tecnología, con políticas públicas para apoyar muchas de estas innovaciones". Se refiere al ejemplo mencionado de neutralidad de la red, donde la regulación es necesaria en el corto plazo, pero a largo plazo es mejor una solución técnica. Otra dificultad que menciona es que las presiones del mercado y otras presiones sociales incitan a las personas, las empresas o las organizaciones a hacer lo que es técnicamente

posible, con independencia de si es legal o no.

Preguntamos si, dada la actual falta de incentivos económicos y del mercado para cambiar la tecnología, será factible dar a los usuarios una mejor seguridad o servicios descentralizados, si no es mediante la legislación y reglamentación. El investigador admite que es una pregunta difícil; de hecho, dice, mientras que muchos productos nuevos que salen ahora pretenden ser seguros, –por lo que en la era post-Snowden, muchas empresas lo ven como un buen argumento para la venta– la verdadera seguridad que ofrecen varía mucho de un producto a otro, al punto que muchas aplicaciones de mensajería supuestamente "seguras", no lo son para nada.

Considera que la salida para las empresas u organizaciones que realmente quieren cambiar el statu quo sería construir soluciones que generen una excelente experiencia de usuario, y luego introducir la seguridad y la descentralización como parte de ella. "No veo ninguna otra forma para que podamos conseguir la aceptación pública que necesitamos para este tipo de soluciones", añade, si bien reconoce que no es fácil hacerlo; sin embargo, ya hay gente que está trabajando en este tipo de soluciones. "Espero que podamos lograrlo, pero no es imposible que podamos fracasar y que el futuro sea de una Internet muy US-céntrica, corpócrata, propagandística, de vigilancia generalizada y totalitaria. Y por extensión, estamos hablando del mundo entero, ya que Internet se está convirtiendo en parte de nuestra vida natural".

Mientras tanto, hay algunos pasos bastante simples que los usuarios ordinarios pueden dar para mejorar su propia privacidad y seguridad (vea el recuadro). "Es muy importante no darnos por vencidos", insiste Ola Bini. "Es una situación sombría pero podemos luchar. No hay que desesperar, sino más bien auto educarnos. Necesitamos más gente que entienda estos temas, que piense al respecto y esté consciente de ellos», concluye.

Consejos para un uso más seguro de Internet

"Nada te puede dar 100% de seguridad", admite Ola Bini, pero para la mayoría de la gente las siguientes medidas, bastante simples, podrían significar una importante mejora. Tal vez no podrán protegerte de la NSA, pero lo harán contra los tipos de riesgos más comunes. (La mayoría de las extensiones recomendadas, una vez instaladas, se ejecutan en segundo plano, de manera que no se tiene que aprender a usarlas).

1) Para usuarios de Windows, cambiar el navegador a Firefox.
2) Instalar las extensiones de Firefox: NoScript y AdBlock. No Script hace posible el control de lo que los sitios web te pueden hacer. AdBlock bloquea la mayoría de los anuncios para que no carguen.
3) El plugin (complemento) Privacy Badger detiene muchas de las filtraciones regulares de privacidad.
4) Tener cuidado con las contraseñas: no es buena la recomendación usual de usar 8 o 9 dígitos o letras difíciles de recordar. Es mejor usar una "frase clave", o sea una cadena de 5 o 6 palabras; es más fácil de recordar y más difícil que otra computadora la pueda descifrar.
5) Utilizar un gestor de contraseñas, como 1Password, LastPass o Keepass, que recuerda tus contraseñas (así, sólo tienes que recordar una). Facilita poder usar diferentes contraseñas para diferentes sitios web, lo que aumenta la seguridad.
6) Instalar el plugin Https Everywhere (para Firefox o Chrome), que asegura el uso del sistema seguro https en todos los sitios web que lo soportan. Así, la mayor parte de tu tráfico de Internet será codificado, y por lo tanto no podrá ser interceptado.

En un nivel más complejo, los usuarios que necesitan mayor seguridad pueden usar TOR (para navegación anónima en la web) o encriptado (cifrado) para el correo electrónico y la mensajería; pero todavía son difíciles de aprender a usar correctamente, sobre todo el encriptado, por lo que es recomendable aprenderlas con ayuda técnica calificada.

¡Haz la ciberpaz, no la ciberguerra!

Prabir Purkayastha

Las armas cibernéticas ya no son cosa de ciencia ficción. Son bastante reales, como también lo es su amenaza a nuestro mundo interconectado. Esta amenaza seguramente crecerá en el futuro cercano con la Internet de las cosas[1], cuando todos nuestros dispositivos serán inteligentes y estarán conectados a Internet. Si queremos impedir que Internet sea militarizada, tenemos que empezar a hablar de lo que los Estados-nación deben o no deben hacer. Y eso significa un pacto internacional a la par de lo que el mundo consiguió para las armas biológicas y químicas, y que no pudo hacer para las armas nucleares.

Aquí hay dos preguntas interconectadas que enfrentamos: ¿vamos a reconocer el peligro que representa el ciberespacio militarizado y enfrentarlo de lleno? ¿O vamos a permitir que se continúe construyendo un mundo en el que unos pocos países, por su poder ofensivo, lleguen a un estado de disuasión mutua, como nos ha sucedido con las armas nucleares, y que nos deja siempre a la orilla de una situación de descontrol, que puede estallar en cualquier momento? La no proliferación no es el desarme, como estamos aprendiendo a costa nuestra.

Peligra nuestra infraestructura vital

Un Estado-nación hoy puede tener la capacidad de atacar a las computadoras que controlan la infraestructura vital de otro país, causando fallas catastróficas. Consideremos el caso de un reactor nuclear. Su núcleo está controlado por computadoras integradas, que son parte del sistema de control del complejo. Si se conoce el sistema de control, es posible "infectar" el sistema de manera que provoque su mal funcionamiento, llegando incluso a una fusión del núcleo. Después de Fukushima, ¿alguien puede dudar de que esto sería un acto de guerra, a la par de un ataque físico contra el reactor nuclear?

La red de energía eléctrica, el control de fábricas peligrosas, las redes de telecomunicaciones, los controles de tráfico aéreo, incluso los aviones en vuelo, son manejados por computadoras y software. Con Internet de las cosas, incluso la humilde lavadora tendrá computadoras incorporadas y estará conectada a Internet. Si los países se plantean jugar con este tipo de software y computadoras, se abre todo un nuevo campo de guerra, con consecuencias incalculables.

En la planta de enriquecimiento de combustible nuclear, en Natanz, Irán, los EE.UU. e Israel desplegaron el virus Stuxnet[2] para atacar a los controladores de Siemens de las centrifugadoras, ocasionando daños físicos a los equipos. Incluso cuando un equipo o país específico es el blanco, Stuxnet ha demostrado[3] que estos virus pueden escapar y propagarse, constituyendo una amenaza para otros equipos y países. El virus Stuxnet infectó a miles de tales equipos en Indonesia, India y otros países, y fácilmente podía haber afectado a

1 Ver http://bit.ly/1aQNj3H

Prabir Purkayastha es co-coordinador de la Coalición Just Net y participa en el Movimiento por el Software Libre de India.

2 Ver http://nyti.ms/1pbStrW

3 Ver http://bit.ly/1KdVaVF

otros controladores de Siemens en los equipos vitales de estos países. El ataque a Irán –con la clave *"Juegos Olímpicos"*– no sólo se dirigió a las centrifugadoras, sino también a los equipos que almacenan datos de la industria petrolera, utilizando un virus (Flame) que parece ser de la misma familia que Stuxnet.

Se han dado ataques, atribuidos por fuentes estadounidenses a Irán, que borraron los datos de dos tercios de las computadoras Armco en Arabia Saudita; ataques similares se han dirigido al sistema bancario de Estados Unidos. *The Intercept* publicó un documento de la NSA[4] que considera que estos ataques son la respuesta de Irán a los ataques contra Natanz y su infraestructura de información petrolera. En otras palabras, Irán respondió con su propia versión de *Juegos Olímpicos*.

El virus Stuxnet es el primer caso conocido del uso de un virus informático para destruir o dañar equipos físicos. Quienes siguen estos temas reconocen que es la primera vez que un país ha atravesado este umbral. Fue el cruce del Rubicón en los ataques cibernéticos.

En el contexto de la utilización de Stuxnet contra Irán, muchos expertos occidentales han argumentado que el uso de un virus informático para paralizar una planta de enriquecimiento de combustible nuclear es mejor que el bombardeo directo. La cuestión aquí no es qué curso de acción es el mejor (y por supuesto, para quién), sino si se trata o no de un acto de guerra. ¿Existe alguna diferencia entre el bombardeo de una instalación y el daño físico con un virus?

Los socios EE.UU. y los 5-Ojos[5] han insertado 50.000 programas de software malicioso –también llamados Computer Network Exploitations (CNE), explotaciones de la red informática– en las redes de casi todos los países del mundo[6]. Se trata de "bombas lógicas", que, al activarse, pueden derribar estas redes. También han infiltrado armas en la red troncal de Internet[7].

¿Qué es el ciberespacio y qué es la ciberguerra?

Como lo demuestra el ejemplo de Irán, ya estamos en las primeras etapas de la guerra cibernética. Bruce Schneier, el decano de la seguridad cibernética, ha dicho[8]: "Estamos en

4 http://bit.ly/1KIRXMu

5 Conformado por EEUU, Reino Unido, Canadá, Australia y Nueva Zelandia.

6 Ver http://bit.ly/1QrmHYe

7 Ver http://wrd.cm/1z2bWGz

8 http://bit.ly/1zVQQV9

los primeros años de una carrera armamentista de ciberguerra. Es caro, es desestabilizador y amenaza el tejido mismo de la Internet que usamos todos los días. La adopción de tratados sobre la ciberguerra, por imperfectos que sean, serían la única manera de contener la amenaza".

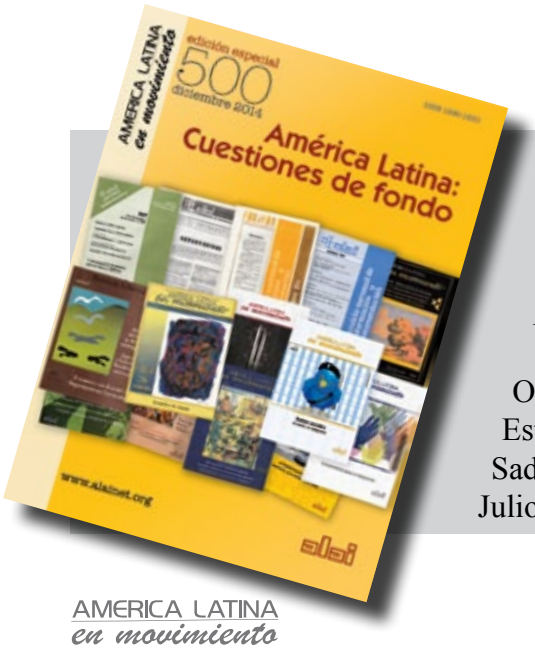
El problema crucial para el desarme en Internet es la convicción de EE.UU. de que está muy por delante de sus rivales, y entonces cualquier pacto de desarme equivaldría a un desarme unilateral. Como resultado, EE.UU. ha rechazado las propuestas de Rusia y China de desmilitarización de Internet, en la ONU y otras plataformas; o les ha diluido al punto tornarlas prácticamente inútiles. Y si bien recientemente ha hecho algunas concesiones -como lo demuestra el Informe del Grupo de Expertos Gubernamentales a la 68ª Sesión de la Asamblea General[9]- por desgracia, se quedan cortas. Todo lo que han logrado es la creación de un nuevo Grupo de Expertos Gubernamentales.

Casi todos los sistemas en el mundo que controlan infraestructura física crítica hoy están conectados a Internet de alguna manera. Pueden estar conectados a través de redes internas que aparentemente están aisladas de Internet, pero en realidad, tienen dispositivos comunes que incumplen este aislamiento. En teoría, se tiene cortafuegos que protegen este tipo de redes internas y sistemas de control. En la práctica, este tipo de cortafuegos de seguridad puede ser fácilmente violado. El ciberespacio es la totalidad de todas las redes y dispositivos que están interconectados de esta manera.

La ciberguerra consiste en ataques en el ciberespacio que traspasan un umbral determinado. Un enfoque para la definición de la ciberguerra sería en términos del daño físico que un ataque cibernético causaría en el mundo real. El ataque, por parte de un Estado contra otro, utiliza el software o código destinado a impedir el funcionamiento (o el mal uso) de una red informática esencial, y así dañar la infraestructura crítica, o causar daño físico a la propiedad o a las personas -incluyendo la pérdida de la vida-, o a ambas. En esta definición, la ciberguerra siempre implica un actor estatal, no es el trabajo de un grupo o un individuo.

Este enfoque tiene el mérito de definir la guerra cibernética como un acto de guerra, sobre una base similar a la definición de un acto de guerra existente en el derecho internacional. Para ser considerado como ciberguerra, las acciones deben estar en una escala que cons-

9 http://bit.ly/1Epbe6o



AMERICA LATINA
en movimiento

América Latina: Cuestiones de fondo
No. 500, diciembre 2014

Osvaldo León, Monica Bruckmann, Oscar Ugarteche, Ana Esther Ceceña, Sally Burch, Raúl Zibechi, Frei Betto, Emir Sader, Irene León, João Pedro Stedile, Eduardo Tamayo G., Julio Fermín

tituye uso de la fuerza (o la amenaza de uso de la fuerza), como lo estipula el artículo 2 (4) de la Carta de la ONU. Otros enfoques pretenden incluir también los daños al sistema informático y a la información, como ciberguerra, lo que requeriría una ampliación de la definición actual de la guerra. Hay, también, el problema de definir qué constituye un umbral: ¿desde qué punto podemos describir la pérdida de información en los sistemas como un acto de guerra? Después de todo, la pérdida de información ocurre por una variedad de razones, apenas algunas de ellas maliciosas.

Sí es posible definir lo que constituye la guerra en el ciberespacio, que permita llegar a un acuerdo internacional que establezca que la ciberguerra –o cualquier ataque que resulte en daño físico o pérdida de vidas– sea en adelante ilegal. Es importante tener en cuenta que el derecho internacional actual no considera todos los actos de guerra como ilegales. Con un margen relativamente estrecho, limita la base jurídica para la guerra, sea a la legítima defensa de un país, o en base a una resolución del Consejo de Seguridad de las Naciones Unidas. Excluir la ciberguerra como una «forma permisible de guerra» en el derecho internacional constituiría un gran paso adelante.

La otra opción sería la de prohibir las armas cibernéticas, con el compromiso, a través de un acuerdo internacional, de que este tipo de armas no vaya a ser desarrollado o utilizado por ningún país. La prohibición de las armas cibernéticas sería similar a la prohibición de las armas biológicas y químicas. Estoy convencido de que, dado nuestra rápida transición hacia un mundo más interconectado, necesitamos ir más allá de la prohibición de la ciberguerra; tenemos que prohibir las armas cibernéticas también. El desarrollo de este tipo de armas es una amenaza para nuestro futuro. Mientras las armas cibernéticas no sean ilegales, existirá la motivación para desarrollarlas como una especie de disuasión. Es más, persistirá la motivación perversa para debilitar la seguridad de las redes y dispositivos.

Las recientes revelaciones de Snowden y otros han puesto de manifiesto que EE.UU. ha debilitado sistemáticamente la seguridad de varias formas. La falta de seguridad fue incorporada a propósito en dispositivos, en el software de los controladores de dichos dispositivos, en distintos protocolos, e incluso en los estándares de encriptación. Las agencias de inteligencia de Estados Unidos lo hicieron en colaboración con los principales fabricantes de hardware y software. Si bien esto puede haber ayudado a la NSA y otras agencias de inteligencia para la vigilancia masiva o dirigida, el peligro es que ha dado lugar a sistemas mucho menos seguros para todos nosotros. Al debilitar los sistemas, la NSA y sus aliados nos han convertido a todos en blancos más fáciles para el software malicioso.

Por supuesto, las capacidades ofensivas son mucho más fáciles de construir que las defensivas. Para lograr una acción ofensiva, solo se necesita tener éxito una vez; para la defensa, se debe tener éxito todas las veces. De ahí que la defensa requiere de la colaboración global. Este es el punto de diferencia con los Juegos Olímpicos: no hay ganadores ni perdedores individuales. Sólo se gana cuando todo el mundo también gana.

Necesitamos un cambio de mentalidad: tenemos que diseñar los dispositivos y las redes con fines defensivos. Tenemos que incorporar la seguridad dentro de la ADN de todas las comunicaciones. Esto significa un cambio de visión de todos los actores, incluido la del actor predominante, EE.UU. Necesitamos construir defensas fuertes y no debilitarlas, si queremos alcanzar la ciberpaz, y no la ciberguerra. *(Traducción ALAI)*

Agradecimientos:

1) Este artículo ha utilizado como fuente, “Apuntes sobre la necesidad de un tratado de ciberpaz”, Coalición Just Net, junio de 2014, disponible en www.alainet.org/es/active/74562.

2) Me gustaría reconocer el aporte de Rishab Bailey, quien hizo gran parte de la investigación para este artículo.

Hacia tierras más libres en Internet

María del Pilar Sáenz

Las empresas prestadoras de servicios de Internet en Latinoamérica están aumentando las ofertas de planes que incluyen acceso a ciertas aplicaciones populares de forma gratuita o que no implican consumo del plan de datos. El *zero rating* llegó a la región y no todos estamos tan contentos.

Zero rating es una práctica bastante criticada por entrar en tensión con el principio de neutralidad de la red, que hace parte de las garantías para mantener Internet libre y abierto. En general, las ofertas tienen como fin aumentar el número de usuarios de Internet con promociones que atraen a un sector muy específico del mercado: el que no tiene mucha experiencia con la tecnología y, por tanto, solo conoce los servicios más populares y los usa para interactuar con herramientas de *social media* al menor costo posible.

En la práctica, cuando no se garantiza el acceso en igualdad de condiciones a todo Internet, empiezan a aparecer problemas como la creación de "jardines vallados" o espacios virtuales donde las empresas tienen el control sobre las aplicaciones o el contenido disponible y la capacidad de restringirlos. Los "jardines vallados" imposibilitan que los usuarios accedan a toda la información disponible, lo que genera un sesgo en su capacidad de tomar decisiones.

María del Pilar Sáenz es física de profesión, activista por vocación. Entusiasta del software libre, de las tecnologías abiertas y de la cultura libre. Trabaja en la Fundación Karisma y es parte del colectivo RedPaTodos y de Hackbo. @mapisaro

También surgen problemas de competencia. Si alguien toma decisiones sobre qué programas, aplicaciones y/o recursos están disponibles, otros muchos quedan por fuera, incluidos competidores directos y nuevas propuestas que no tendrán manera de llegar a sus usuarios potenciales.

Un tercer problema es la afectación cultural. En los últimos 30 años, han emergido una serie de culturas alrededor de la red, que han luchado por mantenerla libre y abierta. Un ejemplo es la llamada "cultura hacker", basada en los principios de la ética hacker: una serie de valores, entre ellos, el libre acceso al conocimiento y la accesibilidad. El trabajo de estas comunidades está en la base de Internet y de todas las grandes empresas que se nutren de este ecosistema. Sin acceso libre a Internet, este ciclo corre el riesgo de romperse y, en lugar de personas curiosas y activas, capaces de innovar, veremos cada vez más simples consumidores pasivos que no diferencian Facebook de Internet.

Uno de los primeros países sobre los que tenemos información del impacto de planes *zero rating* es Paraguay, en donde Tigo, en alianza con Facebook, ofrece desde hace más de un año un plan de Facebook gratuito. De esta alianza habló Mark Zukerberg en febrero de 2014 durante el Mobile World Congress 2014 en Barcelona: "En Paraguay estamos trabajando con Tigo, y ellos también vieron que el número de gente usando datos de la Internet creció en un 50% durante el tiempo de la asociación".

En 2015, el caso icónico para la región es Co-

lombia, en donde Facebook, en asociación con el gobierno del presidente Juan Manuel Santos y, de nuevo, a través de un acuerdo con Tigo, concertó la primera implementación en la región del programa Internet.org. Siguiendo la información de su página web, Internet.org es una iniciativa impulsada por Facebook que "aglutina a líderes en tecnología, organizaciones sin fines de lucro y comunidades locales para conectar a los dos tercios de la población mundial que no cuentan con acceso a Internet".

En Colombia, Internet.org ofrece el acceso gratuito a 16 sitios web: 1doc3, 24 Symbols, AccuWeather, Agronet, BabyCenter & MAMA, Facebook, Girl Effect, Instituto Colombiano para la Evaluación de la Educación, Messenger, Mitula, Para la Vida, Su Dinero, Tambero.com, UNICEF, Wikipedia y YoAprendo. El lanzamiento del proyecto contó con la presencia del creador de Facebook. Pese a que se trataba de dar acceso a unas cuantas aplicaciones, los comunicados de prensa del gobierno y los grandes medios de comunicación anunciaron esta iniciativa como una que busca brindar acceso a Internet.

Semanas después, en el Mobile World Congress 2015 en Barcelona, Zuckerberg indicaba que "el 50 por ciento de los usuarios de datos en Colombia se han beneficiado con Internet.org". No hay cifras oficiales que nos permitan contrastar esta afirmación. De ser así, significaría que en este momento la mitad de los usuarios de datos en Colombia no están accediendo a Internet, sino a una versión limitada y desdibujada de la red a través Internet.org.

No sabemos cuáles serán los siguientes países de la región en acoger Internet.org como parte de sus políticas de Estado. Aunque en septiembre de 2014 Zukerberg adelantó gestiones con el gobierno de México, a la fecha no hay ningún anuncio oficial. Sin embargo, en marzo de este año se comentó que para 2015 dos nuevos países de América Latina entrarán en Internet.org.

Lo que sí existe en este momento es una proliferación de planes y ofertas que incluyen accesos gratuitos a algunos servicios. En Perú hay ofertas de WhatsApp gratuito por parte de Claro. En México, Telcel mantuvo una promoción de WhatsApp gratuito desde agosto hasta diciembre de 2014 y ahora es Movistar quien ofrece un plan que diferencia el acceso a redes sociales (Facebook, Twitter, WhatsApp) y correo al resto de Internet. En Paraguay, Tigo mantiene la promoción de Facebook y WhatsApp gratis. En Colombia, además de Internet.org, los operadores también ofrecen WhatsApp gratis.

Como ya se había planteado, estos planes, promociones e implementaciones basados en prácticas de *zero rating* generan diversas tensiones con la neutralidad de la red. Por eso, para los defensores de estos modelos, el desarrollo de regulaciones y políticas públicas alrededor de la red podrían representar un obstáculo.

De los países de la región, Chile es el único que se ha pronunciado sobre el tema de forma clara y contundente. La Subsecretaría de Telecomunicaciones advirtió a las empresas de telecomunicaciones que, en su interpretación sobre la ley de neutralidad, aquellas ofertas

comerciales que aseguran la gratuidad en el uso de aplicaciones de redes sociales específicas (u otras), como WhatsApp, Facebook, Twitter, poseen un carácter eminentemente discriminatorio al beneficiar a una aplicación específica en desmedro de su competencia. Así, la única forma en que los operadores chilenos pueden ofertar planes de *zero rating* es si la gratuidad se aplica a todos los oferentes de contenido de la misma clase. Esto supondría que si un operador en Chile quiere ofrecer WhatsApp gratis también deberá ofrecer Telegram, Line, Viper y cualquier otra aplicación similar.

Los demás países aún no se pronuncian. En el caso colombiano, la neutralidad de la red admite en su definición la segmentación de mercado. En la interpretación tomada por el organismo de control –es decir, la Comisión de Regulación de Comunicaciones–, los operadores pueden ofertar planes siempre que pongan a disposición de sus usuarios una alternativa o plan tarifario que no contemple limitación alguna respecto de los servicios, contenidos o aplicaciones a los cuales puede acceder el usuario. Una interpretación de la neutralidad de la red que difiere bastante de la chilena y que supone que en Colombia tengamos planes gratis de "WhatsApp" o "Internet.org", o planes tarifarios económicos para "chat" o para "redes sociales", donde el operador define qué servicios incluye.

En Brasil, aún está en discusión la reglamentación del Marco Civil de Internet. Se espera que el tema de *zero rating* haga parte del debate sobre neutralidad de la red en ese país.

Mientras los debates y determinaciones de los países toman forma y se mantienen las discusiones internacionales sobre el tema en los diversos foros relacionados sobre Internet, las protestas que provienen de los mismos usuarios no se quedan atrás. Se han escuchado algunas voces en la región en desacuerdo con el *zero rating*.

En Colombia, Carolina Botero, de la Fundación Karisma, afirmó que "Internet.org no es Internet". En el caso mexicano, se vio con preocupación la inclusión del tema de segmentación de mercado dentro de la discusión de neutralidad de la red en la reforma de la Ley Telecom. Se plantean dudas en Brasil sobre la conveniencia de este tipo de implementaciones. En este sentido, advierten sobre la creación de "castas" en Internet y lo que supone en términos de rupturas frente a un proceso de inclusión digital.

A mi juicio, una de las reacciones más curiosas es la paraguaya. En ausencia de un marco legal que lo limite, la respuesta ha sido desde lo tecnológico. Un desarrollador paraguayo ha creado un programa que establece un túnel desde Facebook que permite navegar por todo Internet, aprovechando una vulnerabilidad en la aplicación del chat de Facebook. En palabras del desarrollador: "Todos nosotros sabemos que Internet es sobre acceder a muchos sitios, etc. Así que sentí que esta campaña [Internet.org] es una limitación seria". Es decir, siguiendo el espíritu de quienes crearon la red, el desarrollador plantea una solución práctica para garantizar que Internet.org no limite el acceso a Internet.

En el fondo, sabemos que el objetivo de las empresas encabezadas por Facebook con Internet.org, no es altruista. Zuckerberg lo dejó bastante claro este año en Barcelona cuando afirmó: "Al finalizar queremos hacer más dinero y conectar a más personas en el proceso". Puede que el tiro les salga por la culata. Y, siguiendo el camino paraguayo, conectar más personas permita que quienes más lo necesiten puedan salirse del "jardín vallado" creado por Internet.org y los demás planes de *zero rating* hacia tierras más libres en Internet.

Artículo publicado inicialmente en Digital Rights - América Latina y el Caribe: http://www.digitalrights-lac.net/es/hacia-tierras-mas-libres-en-internet/

Neutralidad de la red por una Internet igualitaria

Parminder Jeet Singh

Los países en desarrollo, incluidos los sectores de esos países que en otros temas están políticamente conscientes y movilizados, hasta la fecha se han dedicado principalmente a cuestiones de acceso básico a Internet, y la calidad o el ancho de banda de la conectividad. Hablar de cuestiones de diseño arquitectónico o gobernanza de Internet es a menudo considerado prematuro, cuando la gente carece del acceso básico.

Aprovechándose de esta apatía, las empresas de telecomunicaciones y las grandes corporaciones de Internet (proveedoras de contenidos y aplicaciones) han escogido los países en desarrollo para comenzar a manipular el diseño esencialmente igualitario de Internet. El objetivo es la creación de oportunidades permanentes de generación de renta a partir de esta infraestructura social, la más importante de los tiempos actuales. Facebook y Google han llegado a acuerdos con proveedores de servicios de Internet (PSI) locales para que los usuarios accedan a sus servicios, libre de costos de transmisión de datos. Esto genera un terreno de juego desigual para los servicios de la competencia, en particular para el caso de empresas de nueva creación u organizaciones sin fines de lucro que no pueden permitirse el lujo de pagar a los PSI para que sus servicios se pongan a disposición sin cobrar por la transmisión.

Parminder Jeet Singh es integrante de IT for Change, de India, ONG que trabaja en la intersección entre tecnologías digitales y cambio social, con un enfoque en la equidad y la justicia social.

Facebook ha dado un paso más al ofertar un conjunto de diferentes tipos de servicios en un paquete llamado Internet.org, que se provee libre de cobros por los datos, en asociación con proveedores locales de Internet. Las grandes empresas de telecomunicaciones, principales proveedores de Internet, también están explorando sus propios modelos de negocio, para proporcionar canales prioritarios –con mejor transmisión y más veloz– a los proveedores de contenido que estén dispuestos a pagar más, a expensas de todo el tráfico restante. A menudo, simplemente bloquean servicios de comunicación como Skype o Viber que compiten con los servicios de voz de las mismas empresas de telecomunicaciones, o cobran más por transmitir estos servicios.

Algunas de estas prácticas ya son comunes en la mayoría de los países en desarrollo. Si se les permite echar raíces, el modelo básico de una Internet igualitaria, que implica dar igualdad de condiciones a todos los contenidos y aplicaciones que vehicula, se desfigurará para siempre. Esto no es sólo una cuestión de equidad dentro de nuestra esfera mediática o comunicativa, si bien ésta es una consideración importante. A medida que la mayoría de sectores sociales experimentan transformaciones fundamentales en el marco del paradigma digital en red, tales distorsiones de fondo en la arquitectura de Internet tienen implicaciones que afectan a toda la sociedad, en términos de qué tan igualitarios o no podrían ser nuestros sistemas sociales emergentes.

La neutralidad de la red es el principio según el cual los PSI deben tratar todos los contenidos, aplicaciones y servicios por igual, y no

priorizar ni perjudicar ninguno de ellos, en relación con los demás. Las empresas de telecomunicaciones tienen una motivación evidente para construir canales de prioridad y cobrar más por ellos. Las empresas dominantes de Internet tienen la motivación para arrendar estos canales de prioridad, utilizando su poderío financiero para suprimir la competencia, que proviene muchas veces de empresas incipientes con pocos recursos. Aunque a primera vista son injustos, tales acuerdos comerciales son comunes en la mayoría de áreas de la economía. Es importante, entonces, entender por qué se requiere de intervenciones reguladoras en relación con Internet, para que aseguren que no haya discriminación por motivos comerciales. Mientras tanto, hay muchos matices en los puntos de vista sobre la neutralidad de la red, e incluso respecto a lo que se entiende por neutralidad de la red. Las grandes empresas de telecomunicaciones y corporaciones de Internet suelen proclamarse defensoras de la neutralidad de la red, aun cuando una mayoría de personas considera que la violan. Lo que quieren decir es que no consideran que algunos tipos de discriminación, aunque sea por motivos comerciales, sean una violación de la neutralidad.

Lo que la neutralidad de la red no es

Por lo dicho, es importante aclarar lo que es realmente la neutralidad de la red y lo que es la base de un principio regulador como este. Se puede empezar señalando lo que la neutralidad de la red *no* es. Aunque a menudo se lo entiende y se lo propone como tal, la neutralidad de la red no es un principio técnico. Tampoco es un principio de libre mercado. Es cierto que la arquitectura inicial de Internet se basó en el principio de que el cable de transporte era completamente tonto, sin capacidad para discriminar entre los bytes que transitaban por él. Toda la inteligencia se ubicaba en la periferia, en los dispositivos en los extremos que recogían los bytes y los ordenaban en patrones inteligibles. Sin embargo, desde hace algún tiempo, existe una considerable inteligencia incorporada en la red, capaz de discriminar entre bytes para muchos propósitos, especialmente para la gestión del tráfico, de manera de asegurar una buena experiencia de Internet para todos los usuarios. Mientras este tipo de discriminación no se hace por razones comerciales, ya sea para favorecer las ofertas propias de un PSI, o la de sus socios comerciales, tal discriminación no se considera como una violación de la neutralidad. Por lo tanto, la neutralidad de la red como principio técnico, se desvaneció. El término es utilizado hoy en día principalmente en el sentido de una intervención reguladora.

A muchas personas les gusta presentar la neutralidad de la red como un principio de libre mercado. Su postura es que se debe permitir que el mercado determine cuáles contenidos / aplicaciones / servicios de Internet tendrán éxito y cuáles no. Las empresas de telecomunicaciones no pueden estar jugando a favoritismos en este plano, pues sería interferir con el libre mercado. A menudo se define a la neutralidad de la red como el derecho del usuario/a (o consumidor/a) a acceder y a usar cualquier contenido, aplicación o servicio de su elección. Pero entonces surge la pregunta de si invocar una intervención regulatoria del Estado que impide muchos modelos de negocio posibles para las empresas de telecomunicaciones, no sería una injerencia en el libre mercado y la libre elección. Después de todo, la mayoría de empresas de telecomunicaciones parecen estar dispuestas hoy a proporcionar una variedad de modelos, incluyendo aquellos con neutralidad de la red (sin duda como resultado de la enorme presión del lobby a favor), como un conjunto de «opciones» para el cliente. ¡De hecho parecería que esto es la mejor manera de fomentar un libre mercado! Por lo tanto, es difícil defender la neutralidad de la red solo a nombre del libre mercado y de la libre elección.

Mucho más que libre elección, la neutralidad de la red es una cuestión de igualdad de oportunidades. Así como el sistema escolar común es un medio social para garantizar que todos los niños y niñas adquieran un cierto nivel de

igualdad de oportunidades, la neutralidad de la red es un intento de garantizar la igualdad de oportunidades para diversos actores sociales que utilizan Internet para muchos propósitos diferentes. Esto sin duda debe beneficiar también a las empresas incipientes de Internet –si bien ciertamente no son la clase más oprimida de personas– como medio básico para garantizar la innovación. Desgraciadamente, el lenguaje invocado en el contexto de la neutralidad de la red es generalmente el del mercado. Para entender el real sentido y significado del principio de neutralidad de la red, es importante reivindicar el anclaje social más amplio de Internet. Se puede considerar que proporciona un "campo de juego" general para conformar y apoyar una gama muy amplia de actividades e instituciones sociales, siendo el mercado sólo uno de ellas. La equidad o la neutralidad de este campo de juego, es decir, Internet, es importante para consumidores, productores e innovadores –los actores del mercado– pero antes que eso, es también muy necesaria para la ciudadanía, para una variedad de relaciones sociales, para la cultura y la democracia.

Argumentos

Una base mucho más idónea para la neutralidad de la red es el principio de "transportador común" que proviene de la regulación de las telecomunicaciones. Tiene antecedentes en muchas áreas del transporte, carreteras y puentes y en los servicios postales. Según este principio, un servicio de transporte debe estar igualmente accesible a todo el "tráfico" susceptible de transitar por él, sin discriminación. La entidad reguladora estadounidense recientemente clasificó a Internet como un servicio de telecomunicaciones, cambiando su anterior clasificación como "servicio de información", a fin de poder aplicarle el principio de transportador común, y así extrapolarlo a la regulación de la neutralidad de la red. Sin embargo, el concepto tradicional de transportador común sí permite, a veces, ciertos tipos de priorización pagada, como es bien conocido en el caso de los servicios postales y de mensajería. Además, es usual ofrecer diferentes modelos donde el costo del transporte puede ser pagado, sea por quien reciba, sea por quien envíe. Una opción como ésta sustenta la muy controvertida práctica de aplicar una "tasa cero" (*zero rating*) para los servicios de Internet. Implica que algunas aplicaciones o servicios seleccionados se ofrecen a los consumidores sin costo de transmisión de datos, ya que más bien es el proveedor del servicio que sufraga los costos a la empresa de telecomunicaciones. Todos los demás servicios también están disponibles, pero con los costos regulares de transmisión de datos.

Fue justamente una oferta de tasa cero de la mayor empresa de telecomunicaciones de la India, lo que actualmente está causando un gran revuelo en el país a favor de la defensa de la neutralidad de la red. Alrededor de 100.000 correos electrónicos se envían a diario al regulador de telecomunicaciones sobre este asunto, sumando un total de más de un millón hasta la fecha. En respuesta a las acusaciones contra ella, hace unos días, esta empresa de telecomunicaciones alegó que nunca priorizará ni obstaculizará ningún tipo de tráfico. Lo que está haciendo es simplemente invertir el papel de pagador, entre el consumidor y el productor, para cierto tráfico de datos. Esto, según argumenta la empresa, no distorsiona el principio básico de neutralidad de la red, puesto que ningún tráfico se prioriza ni se obstaculiza. Todavía no está claro si la nueva regulación de neutralidad de la red en EE.UU. prohibirá tales prácticas de tasa cero. Al parecer, aquí se necesita algo más que el principio de transportador común aplicado en los sectores de comunicación y transporte de datos, si vamos a mantener una Internet realmente libre de discriminación.

De hecho, hoy Internet es mucho más que un simple canal de comunicación. Para empezar, se la reconoce universalmente como una nueva forma mediática. Además del principio de transportador común, la aplicación de algunos de los principios regulatorios de los medios de comunicación a este nuevo medio podría permitir una buena base para proteger y pro-

mover su carácter público no discriminatorio. El ámbito mediático es reconocido como un sector de importancia social tan excepcional, que es usual no sólo prohibir varios tipos de discriminación, que podrían ser tolerados en servicios comerciales regulares, sino también imponer controles a la integración vertical (por ejemplo, entre los niveles de portador y contenido), límites a la propiedad cruzada entre tipos de medios o de plataformas, la clara separación entre contenido editorial y comercial, la discriminación positiva para proteger las diversidades de varios tipos, y así sucesivamente. Sería pertinente extrapolar a Internet algunos de estos principios reguladores propios del espacio mediático, para identificar qué tipo de regulación sirve mejor el interés público, y cómo Internet puede ser realmente neutral e igualitaria, asegurando equidad para todos y todas.

Falsa dualidad: empresas buenas y malas

Mirar a Internet a través de un lente mediático nos trae a consideración su "neutralidad" y carácter público en los niveles[1] que están más allá de la infraestructura o de las compañías de telecomunicaciones. Muchos "entusiastas de Internet" argumentan que se necesita reglamentación en el nivel de telecomunicaciones, mas no en los niveles superiores –de aplicaciones o contenidos–. Las tendencias singulares de monopolio en el nivel de las telecomunicaciones, son dadas como la razón primaria. Hay algo de verdad en esta afirmación, puesto que el negocio de las telecomunicaciones implica gran cantidad de costos iniciales, a la vez que la relación ingresos / costos declina bruscamente mientras haya más jugadores compitiendo. Esto nos permite entonces plantear un principio claro en base al cual las necesarias decisiones regulatorias pueden formularse: **cualquier nivel de Internet que exhibe significativas tendencias monopólicas puede requerir regulación para asegurar una apropiada neutralidad para y entre actores y actividades que usan ese nivel**. Esto es necesario porque Internet tiene una relevancia tan fundamental para las estructuras sociales emergentes que no puede ser dejada solamente a las fuerzas del mercado. Cualquier postura reguladora que concierne a Internet necesita, por lo tanto, ser adoptada sobre la base de este claro principio, destinado a servir el interés público. Es importante ir más allá de la noción simplista de "odiar a las empresas de telecomunicaciones, amar a las compañías de Internet", que a menudo caracteriza el discurso popular sobre neutralidad de la red. Actitud sin duda alimentada por el manejo de la percepción pública que realizan las compañías multinacionales de Internet, aunque tiene además bases tanto ideológicas como geopolíticas, sobre las cuales no es posible adentrarnos en este artículo.

Las empresas de telecomunicaciones, sin duda, ocupan una muy significativa posición de "portero" (control de acceso). Han mostrado una propensión a actuar en forma oligárquica en el caso de sistemáticas violaciones de la neutralidad de la red, siendo que las fuerzas del mercado por sí solas no pueden frenar estas distorsiones. *Es justamente por ello* que es importante obligarlas a cumplir con la neutralidad de la red. Sin ella, gran parte del potencial igualitario de Internet se perderá, y las estructuras sociales emergentes, con soporte digital, estarán inherentemente más desiguales incluso que las actuales, que ya son bastante malas. Sin embargo, hay que tener en cuenta que también existen características monopólicas muy significativas en otros niveles de Internet, que son igualmente básicas para asegurar un "campo de juego digital" equitativo. En consecuencia, una regulación apropiada podría ser requerida también para estos niveles superiores de Internet, para mantenerlas suficientemente abiertas y evitar posiciones rentistas.

¡Es mucho más difícil hoy que las personas

1 NdE: Los sistemas de transmisión de Internet se organizan en niveles (o capas) superpuestos, desde el nivel físico hasta el nivel de aplicación (cada nivel depende de los inferiores). Aquí el autor se refiere a niveles que van desde la infraestructura hasta las aplicaciones y los contenidos.

puedan cambiar de proveedor de las aplicaciones predeterminadas, sea de las redes sociales (Facebook), los medios de comunicación instantánea (Twitter), la mensajería (WhatsApp) y el trabajo del conocimiento ("el entorno Google»), que cambiar de proveedor del servicio de telecomunicaciones! (Esto es especialmente cierto para lugares donde la portabilidad numérica es obligatoria, gracias a la regulación, como en India). Subyacente a este hecho, hay una muy interesante narrativa que se pierde en el actual debate sobre neutralidad de la red, que a menudo se presenta como una especie de enfrentamiento entre los "malos" explotadores del sector de telecomunicaciones, de un lado, y los "liberadores" del sector empresarial de Internet, de otro. (¿El mismo sector privado de las telecomunicaciones no era el héroe de la "revolución móvil" en los países en desarrollo, hasta hace solo unos pocos años?)

Derechos de las personas e igualitarismo

Mantener Internet neutral es sumamente importante, ya que se está convirtiendo no sólo en la infraestructura, sino en la matriz de una multitud de actividades sociales, como también de las organizaciones e instituciones de la sociedad. No sería redundante decir que estamos avanzando hacia una sociedad mediada por Internet. En cualquier sociedad, es la decisión política la que determina qué aspectos se consideran como los asuntos, sectores o condiciones del campo de juego, para los que se debe garantizar un cierto grado de equidad a través de políticas o regulaciones, y cuáles son considerados las "áreas de juego" donde la gente puede competir y en consecuencia "ganar" (o perder) la asignación de recursos. Tradicionalmente, la gobernanza, la justicia y la seguridad básica se consideran áreas del "campo de juego", al igual que la educación básica, la salud, y una cantidad creciente de lo que se entiende como derechos de las personas. La cuestión de si se considera necesario asegurar que ciertos servicios básicos de Internet se provean equitativamente para todos y todas –no solo como consumidores de servicios, sino también como productores, partícipes, innovadores, ciudadanos, etc.– es, por lo tanto, una decisión sociopolítica, que depende de qué tipo de sociedad queremos. Estas consideraciones sociopolíticas están en la base del principio regulador de la neutralidad de la red. En consecuencia, sería apropiado ubicar Internet en un marco basado en derechos, no solo de derechos negativos como la libertad de expresión y la privacidad, sino también de derechos positivos como el acceso universal y cierto grado de neutralidad básica e igualdad en Internet.

En suma, la neutralidad de la red no es ni un principio técnico, ni algo necesario para sostener el libre mercado. Es un principio igualitario, aplicado a un pilar fundamental y determinante de nuestros nuevos sistemas sociales: la Internet. Es necesario hacer cumplir este principio si vamos a encaminarnos hacia sociedades más igualitarias. Es menester preservar y promover la lógica de la horizontalidad e igualdad que hizo de Internet una fuerza tan desestabilizadora, no solo en la esfera económica, sino también en los ámbitos político, social y cultural. Es igualmente importante frenar las múltiples tendencias de acelerada centralización de poder en tantas áreas, que resultan de la lógica social de las redes. Pero para poder garantizar estas metas, los principios de neutralidad, no discriminación y equidad deben aplicarse de manera consistente y meticulosa para todos los niveles de Internet. La lucha clave hoy tiene que ver con la neutralidad del nivel de infraestructura o de telecomunicaciones, en comparación con los niveles superiores de aplicaciones, contenidos y servicios. Sin embargo, luchas similares se requerirán para enfrentar los monopolios, acuerdos amarrados y estructuras rentistas en estos niveles superiores. En consecuencia, ahora es importante movilizar todas las fuerzas posibles a favor de la neutralidad de la red, pero hay que tener cuidado de no hacerlo bajo las banderas de los Googles y Facebooks de este mundo (si bien ciertamente se pueden considerar alianzas tácticas). ¡Necesitamos mantener nuestra pólvora seca para el día en

que nos movilicemos para enfrentar a los Googles y Facebooks, y asegurar la neutralidad en los niveles que ellos monopolizan!

Considerar la neutralidad de la red como un principio igualitario nos ayuda también a evitar posiciones "técnicas" extremas –como tratar de imponer algún tipo de estricta neutralidad, incluso cuando podría ser claramente contraria al interés público–. Es posible que sostener el interés público podría, a veces, requerir una discriminación positiva a favor de algunas aplicaciones, contenidos y servicios. Esto puede no equivaler a una violación de la neutralidad de la red, de la misma forma en que la reserva de puestos de trabajo para mujeres no se considera discriminación de género. A medida que los teléfonos móviles conectados a Internet se vuelven casi omnipresentes, incluso en los países en desarrollo, es muy posible que los gobiernos implementen y promuevan un canal de datos de tasa cero para algunos servicios esenciales para la ciudadanía, que podría facilitar, por ejemplo, su participación en debates y decisiones públicas trascendentes. Del mismo modo, siendo probable que Internet se convierta en una plataforma clave, cuando no la principal, para los medios comunitarios, podría ser útil explorar canales exclusivos para la radio y televisión comunitaria local, incluyendo la posibilidad de cobros de datos de tasa cero. Tales posibilidades pueden ser puestas en vigencia por el regulador a través de las condiciones de licencia para las empresas de telecomunicaciones. Medidas como estas contribuyen a reforzar la no discriminación o la neutralidad en Internet, al mitigar las desigualdades y discriminaciones incorporadas en las estructuras sociales en general. La discriminación positiva en Internet para el interés público, determinada por mecanismos debidamente legitimados, encaja en la definición de neutralidad de la red que prohíbe cualquier discriminación por parte de los "proveedores de infraestructura", por cualquier motivo de intereses comerciales, entre las diferentes aplicaciones, contenidos y servicios. *(Traducción ALAI)*

Mujeres en Internet

Visibilidad para afianzar reconocimiento y derechos

Dafne Sabanes Plou

Mucho ha sucedido en materia de desarrollo tecnológico y de usos del ciberespacio desde que el movimiento de mujeres comenzó a apropiarse de Internet y de las tecnologías de la información y la comunicación. El trabajo en red, que se afianzó en la década del '90, conectando a organizaciones de todo el mundo, y los usos estratégicos de las tecnologías para acceder a información, elaborar contenidos y luchar por los derechos de las mujeres, que tomó forma a comienzos del nuevo siglo, fortaleció rápidamente al movimiento mundial de mujeres, otorgándole visibilidad y voz en el debate público.

Al adoptar las tecnologías para su comunicación, ellas conectaron el activismo con el trabajo por sus derechos, dando a conocer públicamente sus opiniones, artículos e investigaciones. También pudieron salir al cruce del discurso predominante en los medios y en los sectores conservadores de la sociedad utilizando espacios visibles, redes sociales y mensajes en teléfonos móviles, para dejar al descubierto los estereotipos y prejuicios anclados en el tiempo y en tradiciones ya superadas por la práctica; y al mismo tiempo, mostrar los logros alcanzados por las mujeres que han transformado su visión y su ejercicio de la ciudadanía también en Internet.

Dafne Sabanes Plou es coordinadora regional para ALC, Programa derechos de las mujeres, Asociación para el Progreso de las Comunicaciones

No obstante, continúan existiendo varias áreas críticas a las que las mujeres siguen prestando atención para lograr una participación plena en la sociedad de la información, con igualdad de oportunidades y equidad en la posibilidad de acceder a los beneficios que resultan de estos nuevos desarrollos.

¿Qué hay sobre los derechos de las mujeres en Internet?

Una de estas áreas críticas tiene que ver con el acceso a una conectividad de calidad y a un uso significativo de las tecnologías. Todavía existe una brecha digital de género que crea una barrera importante en el acceso a la economía basada en la tecnología. A no ser que las mujeres tengan un acceso equitativo a Internet, perderán oportunidades de trabajo y de obtener mayores ingresos, de producir y vender en los nuevos mercados que surgen en línea, de acceder a información, lograr nuevos contactos, mejorar su nivel educativo y participar en los procesos de toma de decisiones que determinan su futuro. Las mujeres necesitan que se tomen en cuenta las barreras que se crean debido al costo de las comunicaciones en Internet, la falta de infraestructura que brinde conectividad de calidad, las pocas oportunidades para capacitarse, entre otras.

Internet se ha convertido en un importante espacio para la discusión y la participación política, donde la conexión entre diferentes actores y actoras, movimientos y organizaciones, ha permitido una articulación significativa de la sociedad civil y la construcción de opinión

pública, con posibilidades de influir en las decisiones políticas, los hechos culturales y en la marcha de la economía. Los gobiernos y las empresas no pueden ya soslayar su importancia y ofrecen servicios de toda índole en línea, como también toman decisiones muchas veces basadas en la reacción del público en las redes sociales. Es imprescindible que las mujeres puedan participar de estas discusiones públicas y puedan asociarse y organizarse para trabajar por sus derechos, ejercer su libertad de expresión y rechazar toda discriminación y exclusión.

Los derechos a la comunicación y, en especial, a la libertad de expresión y de información de las mujeres, se han constituido en aspectos claves para el logro de su autonomía, tanto personal, como económica, y para la participación en las decisiones. En Internet las mujeres encuentran espacios para dar a conocer sus prioridades, discutir posicionamientos y para articular su propio discurso, lejos de la perspectiva de los medios que continúan muchas veces tratándolas como objetos, víctimas o como sólo capaces de desempeñar roles secundarios en el mundo del trabajo y la economía. En muchos temas, las mujeres ya han dejado de no tener voz y, por el contrario, sus aportes al debate público han ayudado a la comprensión de que se puede convivir en una sociedad que respete la diversidad y apunte a democratizar las relaciones cotidianas y sociales en todos los ámbitos.

Barreras

Las barreras que las mujeres deben sortear en el ciberespacio tienen que ver con aquellas que son difíciles de eliminar también en el mundo real. En los últimos años se ha visto un aumento de la violencia contra las mujeres en Internet, no sólo como una continuación de la violencia cotidiana y los juegos de poder ejercidos por sus parejas o ex-parejas, sino también intentos de censurar, acallar voces, suprimir demandas y provocar el abandono del activismo por los derechos de las mujeres.

En una encuesta[1] realizada por la Asociación para el Progreso de las Comunicaciones -APC- en 2013 entre activistas de derechos sexuales, en su mayoría mujeres, el 99% de las personas que respondieron reconoció que Internet es una herramienta crucial para el avance de su trabajo por los derechos humanos. No obstante, 51% dijo haber recibido amenazas en línea debido a su activismo. Un tercio mencionó intimidación (34%), otro número similar dijo haber sufrido bloqueos y filtrados de sitios y mensajes (33%) y un porcentaje apenas menor (29%) mencionó haber sido censuradas. Debido a esto, un 27% de las personas consultadas admitió haber discontinuado la labor que realizaba en línea.

Hackeos de cuentas y de sitios web, agresiones de trolls en foros y redes sociales, vigilancia, hostigamiento y acoso son algunas de las conductas violentas que persiguen a las activistas en Internet, en las redes sociales y en los teléfonos móviles. La destrucción de información, el robo de bases de datos, el control en línea de las actividades de las militantes por los derechos de las mujeres, ya se han convertido en situaciones que se denuncian casi a diario. A veces los trolls son hombres misóginos que quieren molestar y destruir, otras veces la vigilancia y el acecho provienen de organizaciones o de servicios paragubernamentales que quieren terminar con toda oposición o cuestionamiento al tratamiento de temas que son claves para las mujeres, principalmente los derechos sexuales y reproductivos.

Ya son muchas las denuncias en América Latina y el Caribe sobre persecución y hostigamiento de defensoras de los derechos de las mujeres que incluyen todo tipo de presiones para socavar su agencia y hacerlas abandonar su militancia. Que la encuesta anterior señale que un 27% de activistas discontinuaron su trabajo en línea por las agresiones sufridas significa una pérdida valiosa y un cercenamiento del compromiso político y social de decenas de personas. Estos hechos deben ser condenados por las autoridades y las corporaciones

1 http://bit.ly/1DZ2RNr

dueñas de las plataformas de comunicación, en especial las redes sociales, quienes deben también brindar soluciones que reparen y den seguridad a las activistas para que no abandonen su compromiso y su labor en los espacios digitales.

El ejercicio de los derechos a la comunicación, también en Internet, es reconocido como habilitador de otros derechos. Para las mujeres que muchas veces se ven restringidas a ámbitos cerrados, como el hogar, la familia o la comunidad pequeña, el uso de tecnologías de la información y la comunicación e Internet les abre numerosas posibilidades de informarse, tomar decisiones y actuar con autonomía, articulándose para alcanzar un mayor cumplimiento de sus derechos. Sostener la democratización de estos espacios es crucial para que las mujeres continúen avanzando.

El desafío democrático en Internet

Norbert Bollow

El concepto de "gobernanza de Internet" es uno de los resultados de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), que se llevó a cabo en dos fases, en Ginebra (2003) y en Túnez (2005). En Túnez, se adopta la siguiente "definición de trabajo" de la gobernanza: "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".

En esta "definición de trabajo" distinguimos dos aspectos principales: uno son las palabras que dan al término "Gobernanza de Internet" su significado, esto es: "desarrollo y aplicación... de principios, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y a la utilización de Internet".

El otro aspecto es una afirmación política sobre quién es responsable de esta "Gobernanza de Internet": "los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivos papeles". Si bien se afirma en documentos derivados de la CMSI que la gobernanza de Internet debe ser "democrática, y hacerse con la plena participación de los gobiernos, el sector privado, la sociedad civil y las organizaciones internacionales", no se ha llegado a explicar cómo el principio de que el gobierno de Internet debe ser democrático puede ser implementado en la práctica.

La afirmación sobre la "plena participación" de todo tipo de partes interesadas puede sonar bien, pero no pasa de ser una buena intención que no se refleja en los hechos: desde mucho antes de la CMSI, y más aún hoy, las empresas privadas del sector Internet, junto con la llamada "comunidad técnica de Internet" de ingenieros (que en su mayoría trabajan para las mismas empresas privadas) son prácticamente los únicos que realmente tienen "plena participación" en la gobernanza de Internet. En gran medida, son los puntos de vista y preocupaciones de este grupo de personas y empresas los que configuran la evolución de Internet y la forma en que se puede utilizar, por ejemplo a través del trabajo del Grupo de Tarea de Ingeniería de Internet (IETF, por sus siglas en inglés).

La gama de puntos de vista es mucho más amplia en algunos foros de discusión (donde no se toman decisiones), como las reuniones anuales del Foro de Gobernanza de Internet (IGF) de la ONU. Sin embargo, no existen mecanismos eficaces para que las prácticas reales de la gobernanza de Internet, -es decir, lo que realmente da forma a la evolución y al uso de Internet-, tengan en cuenta la variedad de preocupaciones que se expresan en el IGF.

Con los actuales mecanismos concretos de gobernanza de Internet, si bien se puede expresar una multiplicidad de puntos de vista -por

Norbert Bollow es consultor independiente en asuntos técnicos y en la solución de problemas empresariales, radicado en Suiza. Participa en el movimiento de Software Libre y de Código Abierto y en otras áreas de defensa de la justicia social relacionada con Internet. Co-coordinador de la Coalición *Just Net*.

ejemplo en el IGF-, cualquier mensaje expresado que no concuerde con los valores propios de los ingenieros de la "comunidad técnica de Internet", simplemente no llevará a ningún resultado concreto en su implementación. Esta situación no es democrática en absoluto. En ausencia de estructuras democráticas formales para la gobernanza de Internet, no hay ninguna manera de hacer avanzar temas de justicia social y económica, ya que no son de interés particular para la mayoría de ingenieros, máxime cuando fácilmente podrían ir en contra de los intereses económicos de sus actuales o futuros empleadores.

Vale aclarar que me refiero literalmente a la palabra "democrática", en el sentido, por ejemplo, de que una elección no es automáticamente un proceso democrático, sino cuando hay una atención adecuada a ciertos parámetros, en particular: (1) cómo se definen las candidaturas, (2) quiénes tiene el derecho de votar, (3) la posibilidad de estas personas de ejercer su derecho al voto, y (4) la prevención del fraude electoral; solo entonces se puede considerar la votación propiamente como una "elección democrática". El significado literal de δημοκρατία (demokratía), en lenguaje moderno "democracia", es que "es el pueblo quien tiene el poder de gobernar". Desde la antigüedad, ello se contrasta con "el imperio de una élite", por lo que el antiguo término griego apropiado para este último es ¤ριστοκρατία (aristokratía). En relación con Internet, la "comunidad técnica de Internet" está jugando el papel de una aristocracia, donde algunas organizaciones son tan poderosas que actúan como los reyes que pueden hacer simplemente todo lo que quieran. Los ejemplos incluyen Google, Facebook, Microsoft y la NSA.

Esto no sería un problema tan grande si Internet tuviera una importancia relativamente menor, como fue el caso en sus inicios. Sin embargo, ahora Internet está facilitando una transición muy significativa de las sociedades humanas hacia un estado de organización mucho más globalizado y mucho más basado en tecnologías digitales, en comparación con todo lo que hayamos conocido antes. Necesitamos asegurarnos de que la democracia, en el sentido literal de la palabra, como se explicó anteriormente, sobreviva a esta transición.

Un gran reto en este plano es que resulta poco atractiva la idea de aplicar directamente a la gobernanza de Internet los procesos existentes de democracia, basados en el Estado (que pueden describirse como implementaciones parciales o totales -de variable calidad- de la idea de la democracia, en el contexto de los Estados-nación).

La idea de la democracia representativa es que, puesto que en el mundo actual, la complejidad general del conjunto de las necesidades de gobernanza es tan grande, la ciudadanía delega las tareas de gobierno a especialistas (el ejecutivo y la rama judicial del Estado) y a un parlamento que supervisa el trabajo del ejecutivo y que por medio de leyes dirige el trabajo del Poder Judicial, o sea, el sistema de las cortes de justicia. Este sistema está en riesgo de ruptura cuando un gran número de ciudadanos no confía en los candidatos de los partidos políticos democráticos que se presentan a elecciones (una situación conocida como "crisis de democracia", que está, por desgracia, extendida, especialmente en muchos países "occidentales"). Además, el sistema democrático basado en el parlamento no puede funcionar en relación con la gobernanza de Internet, cuando ninguno de los partidos políticos mayoritarios propone candidatos al parlamento que tengan un conocimiento real y competencias en esta área. Cuando los políticos no logran demostrar una competencia digna de confianza, prevalecerá el populismo desatinado.

Parte del problema es que en la actualidad resulta muy difícil adquirir cualquier comprensión y competencia en el área de la gobernanza de Internet que no se base en el sistema de valores de la "comunidad técnica de Internet" y en la ideología de "la gobernanza de múltiples partes interesadas" (o multisectorial), que esencialmente trata de preservar las es-

tructuras de poder existentes en la gobernanza de Internet.

Por ejemplo, para las personas que tienen interés en aprender sobre la gobernanza de Internet, un referente importante es la Corporación de Internet para la Asignación de Nombres y Números (ICANN) que, además de algunos asuntos técnicos profundos, que no son directamente visibles para los usuarios finales, decide acerca de la creación de nombres de dominio del nivel superior como ".shop" o ".pharma" y sobre las reglas que se aplican a este tipo de nombres de dominio. Uno de los peligros es que los registradores de nombres de dominio deben firmar un contrato con ICANN (entidad registrada bajo la ley estadounidense) que podría extender algunos aspectos desafortunados de la ley estadounidense al ámbito global.

ICANN, que tiene cuantiosos recursos económicos, utiliza su dinero para atraer a una gran cantidad de personas a sus procesos. Mientras que (a diferencia de algunos otros procesos de gobernanza de Internet) los asuntos no técnicos sí pueden ser colocados como tema de discusión, en los hechos toda la estructura de ICANN está dirigida a asegurar que se tomen las decisiones necesarias en relación a la asignación de "nombres y números". El nombre de la ICANN no es un engaño, su alcance está realmente limitado a esto. Por supuesto, las personas y organizaciones a quienes he descrito anteriormente como una especie de aristocracia, tienen interés en que se siga prestando esta función de gobernanza. Desde su perspectiva, tienen mucho menos importancia las decisiones sustantivas que se tomen en esta institución de gobernanza, que el hecho de que, de alguna manera, se tomen efectivamente decisiones, y que sus resultados sean ampliamente aceptados, nos guste o no.

Ni ICANN, ni cualquier otro proceso establecido de gobernanza de Internet, ofrece oportunidades para suscitar la discusión sobre preocupaciones generales de justicia social y económica en relación con Internet, ni para iniciar el correspondiente proceso de solución de problemas. Esto no debe sorprendernos: después de todo, quienes actualmente detienen mucho poder en el ámbito Internet no tendrían nada que ganar, y, potencialmente, tendrían mucho que perder, con el empoderamiento de los movimientos por la justicia económica y social. Así, actualmente, sólo se resuelven los problemas técnicos y de negocios.

Solucionar problemas reales

En mi opinión, hay tres cosas que se pueden y se deben hacer con el fin de superar este impasse, relacionado con la actual falta de procesos de resolución de problemas de justicia social y económica, relacionados con "la sociedad de la información":

En primer lugar, tenemos que insistir, en cada oportunidad que corresponda, en la solución de problemas reales. Prolongar eternamente las discusiones simplemente no basta.

En segundo lugar, tenemos que crear un espacio donde se pueda desarrollar un discurso de alta calidad, enfocado en la solución de problemas socio-económicos, sin interrupción por parte de quienes preferirían que los problemas de justicia social y económica permanezcan sin resolverse. En mi opinión, el Foro Social de Internet debe ser diseñado de manera que pueda cumplir esta función.

En tercer lugar, tenemos que vincular directamente este trabajo de solución de problemas a la política seria, y específicamente al discurso político presente en los parlamentos. De esta manera, los y las miembros de los Parlamentos serán informados acerca de lo que realmente importa en la gobernanza de Internet. Como consecuencia, el discurso político hegemónico en los medios de comunicación, que presta mucha atención a lo que sucede en los parlamentos nacionales, también estará mucho mejor informado. *(Traducción ALAI)*

CMSI + 10: temas, actores, qué esperar

Richard Hill

¿Qué es la CMSI + 10?

La Cumbre Mundial sobre la Sociedad de la Información (CMSI)[1] fue una reunión de jefes de Estado que se llevó a cabo en 2003 y 2005. Inicialmente se consideró centrarla en acuerdos respecto a los medios y modalidades para aportar al desarrollo de la sociedad de la información, en particular cómo facilitar el despliegue y la aplicación de tecnologías de la información y la comunicación (TICs) en los países en vías de desarrollo[2]. Pero, debido a la falta de voluntad de los países desarrollados para contribuir financieramente a ello, y a la decisión unilateral de Estados Unidos de mantener su control sobre la gestión de los nombres de dominio y direcciones de Internet, gran parte de la discusión giró sobre la cuestión de la gobernanza de Internet, un tema polémico[3].

A pesar de las diferencias de opinión con respecto a la gobernanza de Internet, se alcanzaron acuerdos en una serie de temas relacionados con el desarrollo de las TICs. Estos acuerdos se plasmaron en la Agenda de Túnez 2005[4].

Desde un primer momento se contempló realizar una revisión de los progresos realizados, y es así que en agosto de 2014, la Asamblea General de Naciones Unidas, en su Resolución 68/302[5], decide implementar una Revisión General de los 10 años.

Independientemente de ello, en febrero de 2013 la UNESCO organiza un *Evento de Revisión de la CMSI + 10*[6], mientras que la Unión Internacional de Telecomunicaciones (UIT) lleva a cabo otro evento de alto nivel en junio de 2014[7], y la UNESCO realiza también, en marzo de 2015, el encuentro *Conectando los Puntos: Opciones para Futuras Acciones*[8].

El resultado del evento de la UIT, convenido tras un proceso multisectorial abierto, se plasma en una declaración, donde se reseñan los avances hasta la fecha, y una visión que perfila las medidas futuras a tomar en el contexto de la Agenda de Túnez. Si bien esos resultados se acordaron por unanimidad, hay quienes afirman que deberían haber incluido posiciones más contundentes en algunas materias, tales como la protección de los derechos humanos, políticas tributarias en la economía digital, reformas a las leyes de derechos de autor, reformas de IANA e ICANN[9], y el reconocimiento de que los principios de la necesidad y la proporcionalidad se deben aplicar

1 http://bit.ly/1ldEtuA
2 http://bit.ly/1DZ4QkT
3 http://bit.ly/1Graf7Y
4 http://bit.ly/1xBDE9x

Richard Hill es Presidente de la *Association for Proper Internet Governance*. Es también consultor independiente y ex alto funcionario de la Unión Internacional de Telecomunicaciones.

5 http://bit.ly/1QrgcVi
6 http://bit.ly/1Ezq4Ju
7 http://bit.ly/1kht7bw
8 http://bit.ly/1FViLI6
9 IANA - Internet Assigned Numbers Authority (entidad que supervisa la asignación global de direcciones IP y otros recursos de Internet, operado por ICANN); ICANN - Corporación de Internet para la Asignación de Nombres y Números.

a las actividades de vigilancia[10]. El evento de la UNESCO de marzo de 2015, también emite una declaración que delinea posibles acciones futuras para el organismo, pero esa declaración no obtiene el consenso de todos los participantes, en particular porque no reconoce explícitamente que la Gobernanza de Internet debe ser democrática[11].

¿Qué problemáticas abarca la CMSI + 10?

La Asamblea General de la ONU decidió que la revisión general en diciembre de 2015 se centraría en las brechas potenciales respecto a las tecnologías de información y comunicación y a las áreas que requieren mayor esfuerzo, así como abordar desafíos, incluyendo la reducción de la brecha digital y el aprovechamiento para el desarrollo de las tecnologías de información y comunicación.

Si bien la «gobernanza de Internet» no consta expresamente en la lista de temáticas (sin duda porque EE.UU. se opone a debatir ese tema en un escenario multilateral), es probable que emerja en el marco de temáticas referidas a «reducir la brecha digital» y «aprovechar las TICs para el desarrollo «, tal como sucedió en la CMSI original.

En cuanto a las cuestiones de desarrollo, es probable que las diferencias de opinión que se han visibilizado en varios foros sobre el desarrollo en general, se repitan: un sector sostiene que la desregulación y la privatización es la mejor solución; el otro que, en ausencia de regulación gubernamental apropiada, la desregulación y la privatización podrían simplemente aumentar las ganancias de las empresas, sin aportar los correspondientes beneficios a la ciudadanía.

La objeción de la Coalición *Just Net* a la declaración resultante del evento *Conectando los Puntos* de UNESCO es un ejemplo de tales puntos de vista divergentes[12].

En cuanto a temas específicos, los que tienen más probabilidades de ser discutidos son exactamente los mismos que fueron identificados en 2005 por el Grupo de Trabajo sobre Gobernanza de Internet: el papel asimétrico de Estados Unidos, el costo relativamente alto de la conectividad para países en desarrollo y la seguridad (que ahora incluye privacidad y vigilancia masiva). Estas cuestiones se han debatido ampliamente durante los últimos 10 años[13]. Si bien los defensores del actual modelo de gobernanza consideran que se han registrado algunos avances, la realidad muestra que no ha habido ningún progreso. Por lo tanto, estos asuntos son propensos a ser discutidos nuevamente en la revisión CMSI + 10 de la ONU.

¿Quiénes son los actores de la CMSI + 10?

Hasta ahora, el proceso de la CMSI ha sido bastante abierto, se reciben aportes de los actores no gubernamentales (empresas privadas y sociedad civil), por lo que los documentos expresan un acuerdo general entre varios tipos de actores. Esta tradición se refleja de cierta forma en la resolución de la ONU de 2014, que establece que la revisión general de la CMSI concluirá con una reunión de alto nivel, de dos días, de la Asamblea General, en diciembre de 2015. Será precedida por un proceso preparatorio intergubernamental que también tomará en cuenta los aportes de todas las partes relevantes involucradas en el proceso de la CMSI; y también decidió invitar a representantes de todos los sectores interesados dentro del proceso CMSI a hablar durante la reunión de alto nivel, así como fomentar la participación de las partes interesadas en la reunión.

Pero queda por ver cómo se reflejará esa tradición en la práctica, debido a que las modalidades de participación de los actores no gubernamentales aún no se han especificado. Es más, el proceso preparatorio, que se iniciará

10 http://bit.ly/1bBbZyv
11 http://bit.ly/1DZ5K0C
12 http://bit.ly/1DZ5K0C
13 http://bit.ly/1Graf7Y

sólo en junio de 2015, será un proceso intergubernamental, encaminado a consensuar un documento final a ser adoptado por parte de todos los gobiernos en la reunión de alto nivel de la Asamblea General. Durante el proceso preparatorio para la reunión de alto nivel, el Presidente de la Asamblea General organizará consultas interactivas informales con todas las partes interesadas de la CMSI, con el fin de recoger sus aportes para el proceso de negociación intergubernamental, pero las modalidades de estas consultas aún no se han anunciado.

¿Qué esperar de la CMSI + 10?

Como se mencionó anteriormente, los debates de la CMSI suelen reproducir los debates que tienen lugar en otros foros, y la división entre los puntos de vista se puede caracterizar como Norte / Sur: países desarrollados versus los países en desarrollo (con los BRICS alineados con los países en desarrollo).

Como ya señalé, gran parte del debate se centra (ya sea abiertamente o bajo la superficie) en torno a Internet, que los países desarrollados ven como un facilitador de crecimiento, cuya continuidad sólo estará garantizada si los gobiernos siguen absteniéndose de intervención. Pero en realidad la telefonía móvil es más importante, en la actualidad, en los países en desarrollo. De hecho, los países desarrollados sí favorecen la intervención en cuestiones de internet, cuando esto se ajusta a sus intereses, en particular el cumplimiento estricto de derechos de propiedad intelectual.

Por lo tanto, es probable que haya un enfrentamiento entre las fuerzas que favorecen un modelo internacional de régimen neoliberal (llamado «modelo de múltiples partes interesadas» o multisectorial, cuando se discutan asuntos relacionados con Internet[14]) –en el que Estados Unidos y sus empresas privadas dominan[15]– y las fuerzas que favorecen modelos democráticos de gobernanza[16].

¿A qué apuntar en la CMSI + 10?

Desde la perspectiva de los movimientos sociales y actores de la sociedad civil que luchan por la justicia social y económica, así como los sectores que desean ver que Internet se convierta en una tecnología desarrollada por la ciudadanía, para la ciudadanía (como es el propósito del Foro Social del Internet[17]), será necesario resistir a las presiones de EE.UU. y sus aliados por imponer modelos de gobernanza que favorezcan sus intereses geopolíticos y geoeconómicos[18]. Asimismo, conviene impulsar acuerdos sobre principios básicos[19] que conlleven a un uso más equitativo y justo de las TICs y a la realización y protección de los derechos humanos[20]. *(Traducción ALAI)*

14 http://bit.ly/1KdgDOB
15 http://bit.ly/1Ezr0h1
16 http://bit.ly/1Fkqbrc
17 http://bit.ly/1I4QaUe
18 http://bit.ly/1zV2Oyi
19 http://www.alainet.org/es/active/72842
20 http://bit.ly/1Hx68rg

Llamamiento de Túnez para la Internet de la ciudadanía

Nosotras y nosotros, participantes del Taller "La organización de un Foro Social de Internet - Un llamamiento a ocupar Internet", realizado en Túnez en el marco del Foro Social Mundial, afirmamos nuestro compromiso con el objetivo común de construir la Internet de la ciudadanía desde abajo y más allá de las fronteras: una Internet en función del interés público y la solidaridad, donde el control esté en manos de la gente; una Internet basada en la dignidad humana, la igualdad, la justicia social, la libertad y los derechos de comunicación de las personas.

Unimos nuestras voces a la convocatoria de celebrar un Foro Social Mundial de Internet, como un espacio para debatir sobre la Internet que queremos y cómo construirla antes de que la revolución del conocimiento y del acceso a la información sea secuestrada irremediablemente por los intereses corporativos y las agencias de seguridad, incrementando el nexo de corrupción entre la política y el dinero.

Hoy en día, Internet se ha convertido en una parte integral y esencial de nuestra vida cotidiana; cada vez más, nuestras actividades se organizan a través de o en torno a los espacios virtuales, las redes, los servicios en línea y las tecnologías de Internet. En torno a la red se ha reestructurado el modo en que vivimos, trabajamos, jugamos y organizamos nuestras sociedades. En muchos aspectos, esto es así incluso para las personas que en la actualidad no tienen acceso directo a Internet.

Al mismo tiempo, nos preocupa constatar cómo nuestros espacios, tanto privados como públicos, están siendo cooptados y controlados en beneficio privado; cómo las corporaciones privadas están transformando la Internet pública en espacios cerrados; cómo manipulan y se apropian de nuestros datos personales; cómo está emergiendo una sociedad global de vigilancia que niega la privacidad; cómo se está censurando la información en Internet de manera arbitraria y se restringe el derecho de las personas a comunicar; y cómo se está militarizando Internet. Mientras tanto, la toma de decisiones en materia de políticas públicas relativas a Internet se mantiene peligrosamente alejada de los mecanismos de la gobernabilidad democrática.

Hacemos un llamamiento a todas y todos quienes comparten estos objetivos, a participar durante los próximos meses en la elaboración del Manifiesto de la Internet de la ciudadanía, con el objetivo de buscar un consenso sobre los principios básicos de una Internet orientada a la equidad social, la solidaridad humana y la justicia.

Internet es una herramienta y espacio de trabajo indispensable para la construcción de las luchas sociales y las interconexiones entre los movimientos. Hacemos un llamamiento a los movimientos sociales y organizaciones reunidas aquí en Túnez a asumir esta propuesta como parte esencial de sus agendas de acción, incluyendo, entre otros, los siguientes objetivos:

Exigimos medidas decisivas para frenar la vigilancia masiva indiscriminada que implementan las corporaciones, agencias de seguridad y gobiernos.

Defendemos la descentralización --en la mayor medida posible-- de las estructuras técnicas, económicas y de manejo de datos de Internet; y el acceso a una Internet basada en el principio de neutralidad de la red como derecho, que debe incluir apoyo a redes comunitarias y a infraestructura pública. También defendemos la libertad de la comunicación para las personas.

Nos comprometemos a explotar la revolución de Internet para construir la solidaridad global entre los movimientos populares, para permitirles compartir experiencias a nivel mundial y aprender unos de otros.

La Internet de la ciudadanía debe ser impulsada ante todo por los pueblos. Una Internet dirigida mano a mano entre las grandes empresas y los gobiernos hegemónicos no representa el interés público. Defenderemos el derecho de las organizaciones de base y movimientos sociales, junto con otros actores de la sociedad civil, a participar en las negociaciones mundiales sobre la gobernabilidad de Internet.

Documento del taller *La organización de un Foro Social de Internet - Un llamamiento a ocupar Internet*, FSM 2015, Túnez, 26 de marzo.

AMERICA LATINA *en movimiento*

revista mensual

ACTUALIDAD Y PENSAMIENTO LATINOAMERICANO

- **Realidad Regional**
- **Procesos Sociales**
- **Problemáticas Contemporáneas**

Un esfuerzo conjunto de analistas y pensadores destacados, organizaciones sociales y ciudadanas, escritores y comunicadores comprometidos con las causas sociales.

Fuente de información imprescindible para líderes de opinión, dirigentes sociales, activistas políticos, centros de estudios y formación, periodistas y medios de comunicación, organismos de desarrollo...

¡SUSCRIBETE!

Tu aporte garantiza la continuidad y calidad de nuestra labor informativa

info@alainet.org • www.alainet.org/revista phtml

ALAI • casilla 17-12-877, Quito, Ecuador • email: info@alainet.org • www.alainet.org