ARTÍCULO

EL DERECHO A LA PRIVACIDAD Y EL INTERVENCIONISMO DE ESTADO EN LA ERA DIGITAL

Hedme Sierra Castro[1]

Resumen

La vigilancia gubernamental es un problema creciente, y las formas de vigilancia amenazan con poner en peligro los derechos a la privacidad y la libertad de expresión. Nadie entiende estos desafíos mejor que las defensoras y los defensores de Derechos Humanos que trabajan para proteger y defender los derechos fundamentales de las personas.

Son muchos los gobiernos que vienen utilizando la tecnología de filtro para bloquear el acceso a internet, redes de telefonía celular o protocolos y servicios en línea específicos para restringir la capacidad de las personas de reunirse pacíficamente, restringiendo las libertades de reunión y de asociación. Las redes sociales, por ejemplo, realzan la libertad humana de congregarse en torno a los temas sociales, políticos y económicos, construir asociaciones y redes, y convocarse para promover y defender los Derechos Humanos.

Las prácticas de intervención a las comunicaciones se remontan a los años 1920. Durante el siglo XVIII y XIX las formas del control social se basaban en la dominación fundamentada en una ideología que podía estar legitimada de diferentes formas pero siempre generaba relaciones de mando y obediencia. La lógica del control social se articula con la finalidad de contener la desviación social y así, detectar peligros latentes que devienen de los grupos peligrosos, y por tanto, deben ser administrados para mantener el orden social.

Con la efervescencia de las redes sociales, esto significa un cambio en las formas de organización social, pues las sociedades contemporáneas junto con sus estructuras social-políticas combinan principios democráticos y actitudes autoritarias de manera simultánea definiendo un nuevo tipo de sociedad, utilizando para ello los avances en las Tecnologías de la Información y Comunicaciones (TIC's). Uno de los aspectos novedosos de este tipo de sociedades que evoluciona a la par del desarrollo tecnológico es la sistematización de las tecnologías, donde fundamentalmente la vigilancia será la estrategia que reemplace progresivamente a la coerción física como un medio para mantener el orden y la armonía de la población.

[1] Ingeniera en Ciencias de la Computación (Universidad Católica de Honduras). Máster en Derechos Humanos y Democratización para América Latina y el Caribe (Universidad Nacional de General San Martín). Actualmente se desempeña como Investigadora por Guatemala para el estudio de los marcos legales nacionales e internacionales que protegen el derecho a la privacidad, y que propician la criminalización, vigilancia y censura digital, en Internet y en las Telecomunicaciones de defensoras y defensores de Derechos Humanos en Guatemala, El Salvador, Honduras y Nicaragua. También se desempeña como coordinadora en ACI-Participa Tegucigalpa, Honduras. Correo electrónico: Hedme.sc@gmail.com

La información y el conocimiento siempre han sido componentes cruciales del crecimiento económico; sumadas al surgimiento de un nuevo paradigma tecnológico organizado en torno a las nuevas tecnologías de la información, hacen que la misma información se convierta en el producto del proceso de producción. En este escenario, las tecnologías de la información juegan un papel de vital importancia en el nuevo contexto ideológico, político y cultural de la dictadura del pensamiento único.

Es así como Internet se convierte en un centro de operaciones para los movimientos sociales desde el cual proponer un espacio contra hegemónico y quebrar el bloqueo informativo y distorsionante de los grandes medios de comunicación, redefiniendo el escenario de la protesta a nivel mundial, articulando sus acciones a través de la información y la fluidez de la comunicación.

El advenimiento de la era digital está generando una redefinición radical del funcionamiento de la sociedad, basado fundamentalmente en la capacidad de intercambio directo y en la libre aportación de contenidos y conocimiento. Defensores de derechos humanos alrededor del mundo están tomando acciones y manifestándose en contra de quienes quieren controlar Internet con violencia y abuso de poder. Ante este escenario, es necesario pues, crear lazos humanos de cooperación global y local para hacer frente a quienes buscan oprimir nuestra privacidad y libertad de expresión.

I. Sociedad de Vigilancia

A. Contexto Histórico

Durante los siglos XVIII y XIX las formas del control social se basaban en relaciones de mando y obediencia, con la finalidad de contener lo que más adelante se conocería como desviación social[2], es decir, la desviación respecto a las normas y expectativas de cualquier sistema social o modo de dominación, ante la cual éste reacciona con un dispositivo de control específico. De esta forma, quienes detentaban el poder detectaban los peligros latentes que devenían de grupos sociales potencialmente peligrosos y que debían ser controlados para mantener el orden social establecido. Cabe explicar que el uso del término desviación social se remonta a la segunda mitad del Siglo XIX en los EE. UU., convirtiéndose en un tema de estudio fundamental dentro de la ciencia de la sociología. En la década de 1960 se comenzó a estudiar la desviación centrando los

[2] Robert K. Merton. *Anomie, Anomia and Social Interaction: Contexts of Deviant Behavior*. New York. New York The Free Press. 1964. P. 213.

estudios en las formas de control e interacción social. La principal aportación teórica de esta escuela de ésta teoría es Howard Becker. La delincuencia, entendida como grupos o sectores peligrosos, es una parte políticamente significativa de un fenómeno social más amplio y complejo, la desviación social.[3]

Hoy en día, con el advenimiento de la era digital, las prácticas de vigilancia masiva se ven facilitadas debido el rápido desarrollo de las tecnologías de la información y de la comunicación (TIC). Y, en este sentido, la vigilancia social se define como el control mediante la utilización de medios tecnológicos para extraer datos personales[4]. Las tecnologías desarrolladas en la segunda mitad del siglo XX juegan, sin duda, un papel significativo en la construcción de nuevas formas de control social lo que representa un cambio en las formas de organización social. Uno de los aspectos novedosos de este tipo de sociedades que evoluciona a la par del desarrollo tecnológico es la sistematización de las tecnologías, donde la vigilancia es, fundamentalmente, la estrategia que reemplace progresivamente a la coerción física como un medio para mantener el orden y la armonía de la población. En este escenario, las tecnologías de la información y de la comunicación juegan un papel de vital importancia en el nuevo contexto ideológico, político y cultural de la dictadura del pensamiento único.

La primera agencia estadounidense dedicada a la intercepción de telecomunicaciones en tiempos de paz fue la llamada Cámara Negra (Black Chamber), creada en 1919 a partir de la reorganización de una sección especializada del ejército, que había desempeñado la misma función durante la Primera Guerra Mundial. Desde sus inicios, la Cámara Negra estuvo dirigida por el criptógrafo Herbert O. Yardley, y su primera gran hazaña fue descifrar el código de comunicaciones que en esos momentos manejaba el gobierno de Japón; esto permitió que Estados Unidos conociera anticipadamente las posiciones japonesas respecto a las discusiones realizadas en la Conferencia Naval ocurrida entre el 12 de noviembre de 1921 y el 6 de febrero de 1922, con el propósito de consensuar un acuerdo entre las más grandes potencias (Japón, Francia, Italia, Reino Unido y Estados Unidos) que limitase el potencial militar y de ese modo evitar otra guerra mundial. Más tarde, en 1929, la Cámara Negra fue clausurada por presión del entonces Secretario de Estado Henry Stimson, quien sostenía que: "los caballeros no leen los

[3] Becker. *Outsiders: Studies in the Sociology of Deviance*. New York. New York The Free Press. 1963. Pp. 1-2, 162.
[4] Gary T. *Marx. Surveillance and Society.* Thousand Oaks , California. Encyclopedia of Social Theory. 2005. Pp 817-822

correos de los demás".[5] Sin embargo, después de la Segunda Guerra Mundial, el gobierno de los Estados Unidos decidió que, en efecto, los caballeros necesitan una red de vigilancia permanente.

Durante la Segunda Guerra Mundial, tanto Estados Unidos como Gran Bretaña desarrollaron amplias capacidades de espionaje. A lo largo de la Guerra Fría, la vigilancia hacia la población fue parte de la vida diaria. Estados Unidos entró de lleno en estas prácticas inmediatamente después de la finalización de la Segunda Guerra Mundial, cuando comenzó a revisar cada telegrama que entraba o salía del país; esta actividad era parte del proyecto *Shamrock*[6]. Éste programa de espionaje comenzó a operar en agosto de 1945 y consistía en la acumulación de todos los datos telegráficos que entraban o salían de Estados Unidos y permitía el acceso directo a la información a través de las tres principales compañías estadounidenses de cable: Western Union, la Compañía Internacional de Teléfono y Telegramas (ITT) y la Corporación Americana de Radio (RCA).

En 1946, un año luego de finalizada la Segunda Guerra Mundial, Estados Unidos, junto con sus cuatro aliados más cercanos: Reino Unido, Canadá, Australia y Nueva Zelanda, construyeron una red de sistemas de vigilancia de comunicaciones digitales de alcance mundial llamado Cinco Ojos (Five Eyes). La alianza de los Cinco Ojos, surge a partir de la estrecha colaboración en materia de espionaje que mantuvieron Estados Unidos y Reino Unido durante la Segunda Guerra Mundial, en particular por el trabajo realizado desde la base militar inglesa Bletchley Park, en la que se realizaron los trabajos de descifrado de códigos alemanes durante la Segunda Guerra Mundial[7], para descifrar los códigos alemanes y japoneses. Actualmente, la Alianza de los Cinco Ojos continúa funcionando en base al principio de compartir información y no espiarse mutuamente. Entre estos países existe un alto grado de cooperación estratégica e intercambio de inteligencia; debido a ese trabajo conjunto el material reunido bajo el régimen de vigilancia de un país se comparte con el resto. La gran distancia que separa a éstos países les permite vigilar la mayor parte del tráfico mundial de Internet.[8]

En Estados Unidos, durante las protestas en contra de la Guerra de Vietnam ocurridas en 1967, que traían consigo el creciente movimiento por los derechos civiles, el trigésimo sexto presidente

[5] National Security Agency. *Pearl Harbor Review- The Black Chamber*. Disponible en: https://www.nsa.gov/about/cryptologic_heritage/center_crypt_history/pearl_harbor_review/black_chamber.shtml
[6] Electronic Frontier Foundation. *Amicus Brief of Experts in the History of Executive Surveillance.* Disponible en: https://www.eff.org/es/document/amicus-brief-experts-history-executive-surveillance

[7] Bletchley Park. *History: Intercept to action*. Disponible en: http://www.bletchleypark.org.uk/content/hist/worldwartwo/inttoact.rhtm
[8] Privacy International. *The Five Eyes*. Disponible en: https://www.privacyinternational.org/?q=node/51

de los Estados Unidos, Lyndon B. Johnson, ordenó a la CIA (Central Intelligence Agency/ Agencia Central de Inteligencia) y al Ejército (U.S.Army) intervenir las comunicaciones para saber si el movimiento pacifista recibía ayuda de cooperantes extranjeros. Más tarde, el FBI (Federal Bureau of Investigation/ Oficina Federal de Investigación) incorporó a esta misma investigación algunos nombres de personalidades norteamericanas a las que se debía vigilar. Finalmente, en 1969, la NSA (National Security Agency/ Agencia Nacional de Seguridad) se hizo cargo del programa de espionaje Minarete, proyecto hermano del Proyecto Shamrock, que interceptaba las comunicaciones de personas que estaban en una lista proporcionada por otras organizaciones gubernamentales como el FBI, la CIA o el Departamento de Defensa de los Estados Unidos, éste proyecto no contaba con supervisión judicial ni tampoco tenía órdenes de interceptación. Esta lista de vigilancia contenía más de 1.600 nombres y estuvo activa desde 1967 hasta 1973. En la lista figuraban algunas personalidades como el boxeador Mohamed Alí y al defensor de derechos civiles Martin Luther King, ambos fueron fervientes críticos de la Guerra de Vietnam.

Terminada la Segunda Guerra Mundial, las potencias que participaron en el conflicto decidieron dividirse no sólo lo que quedó de Europa, sino ciertas regiones del mundo. Por ejemplo, Estados Unidos quedó a cargo del control de América Latina, y para ello respaldó gobiernos que fueran adeptos a sus intereses. De esta manera, el continente se plagó de dictadores, producto de golpes de Estado militares que fueron apoyados por el gobierno estadounidense. Así, surgieron líderes dictatoriales que se caracterizaron por impulsar una política que educara a la población a través de una intensa propaganda gubernamental en valores nacionalistas, donde pensar individualmente era visto como una traición a la sociedad.

B. La creación de la red de redes

Para avanzar en el desarrollo de éste tema, es necesario comprender que existen grandes razones políticas que fueron abriendo paso a la expansión y desarrollo de internet, y también de las telecomunicaciones. Luego de la Guerra Fría, en 1958, el Gobierno de Estados Unidos creó la Agencia de Proyectos de Investigaciones Avanzadas para la Defensa (DARPA), y realizó investigaciones que impulsaron la creación de redes que generaron un primer esbozo de internet en 1969, denominado ARPANET (Red de Agencia de Proyectos de Investigación Avanzada/ Advanced Research Projects Agency Network), y fue creada a solicitud del Departamento de Defensa de Estados Unidos como medio de comunicación para los diferentes organismos del país.[9] El primer nodo[10] se creó en la Universidad de California, Los Ángeles (UCLA) y fue la

[9] DARPA. *History*. Disponible en: http://www.darpa.mil/About/History/History.aspx

espina dorsal de internet hasta 1990. A ésta red se conectaron cuatro computadoras situadas en la UCLA, el Stanford Research Institute y la Universidad de Utah respectivamente. Durante esos años se reforzaron las redes y, en 1989, se creó el WWW (World Wide Web, Red Mundial).

Hace casi 30 años, internet ingresó a territorio Latinoamericano en el marco de experimentos académicos, muchas veces inconclusos. Estas conexiones eran temporales y realizadas a través de una línea telefónica. El desarrollo de internet y de las telecomunicaciones en la mayoría de los países latinoamericanos no fue pensado desde una perspectiva federal, soberana y de desarrollo. Los gobiernos estuvieron ausentes y la empresa privada determinó las conexiones, que se fueron uniendo a la red central desplegada desde Estados Unidos.

C. La Sociedad del "Gran Hermano"

En 1949, George Orwell escribió *1984*, una de sus grandes obras literarias en la que vislumbró una sociedad controlada y vigilada por un Estado antidemocrático, donde hace una profunda crítica de los regímenes autoritarios, sus medios de comunicación y la falta de libertad individual. En su obra, el autor introduce el término *Gran Hermano*, con el cual conceptualiza una sociedad supeditada a controles que se encuentran fuera de su alcance, y visualiza la información como el pilar fundamental en toda relación de poder. En otras palabras, la obra sostiene la tesis que el estado ha conseguido el control total sobre el individuo, donde las fuerzas militares y policiales eran instrumentos de ese control social.[11] Con la tecnificación, esos controles fueron superados virtualmente.

Sesenta y dos año más tarde, en 2011, con la efervescencia y apogeo de las redes sociales, el periodista australiano creador de Wikileaks, Julian Assange acuñó el término Gran Hermano de Orwell para denunciar que Internet se encuentran bajo la mirada de los servicios secretos norteamericanos, haciendo fuertes críticas contra Facebook y también contra los más grandes buscadores en Internet: Google y Yahoo. Asimismo, Assange, denunciando que los datos de usuario de estos sitios podían encontrarse ya dentro de los archivos de la CIA. Y luego, en 2013, Assange denunció que Internet ha sido ocupada militarmente por Estados Unidos y sus aliados para dominar a las sociedades atentando contra su soberanía nacional. A los esfuerzos de Assange por difundir documentos filtrados de las bases de datos gubernamentales con la clasificación de *ultra secret,* se suma el ex técnico de inteligencia de la Agencia Central de

[10] Punto de intersección, conexión o unión de varios elementos que confluyen en una misma red, donde cada computadora es un nodo, y en Internet, cada servidor constituye también un nodo.
[11] George Orwell. *1984.* Barcelona. Ediciones Destino. 2009.

Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA), Edward Snowden. Definitivamente, las revelaciones de Assange y Snowden afectaron los mismos intereses.

En junio de 2013, el periódico *The Guardian* publicó la primera de una serie de revelaciones de Snowden[12] sobre el espionaje masivo de Estados Unidos, evidenciando la magnitud, los objetivos y los métodos con los que la NSA, que es la organización de vigilancia más grande y secreta de Estados Unidos, recopila información en todo el mundo. Esto marcó un hito en la conciencia global acerca de la existencia de un aparato mundial de espionaje. El primer documento revelado por Snowden fue una orden del Tribunal de Vigilancia de Inteligencia Extranjera de Estados Unidos (FISA) el cual solicitaba a la empresa de telefonía Verizon entregar todos los registros detallados de las llamadas telefónicas realizadas desde Estados Unidos hacia el extranjero, y también las llamadas locales. Esta autorización también permitía a la NSA recolectar información de inteligencia de organismos como el Banco Mundial, el Fondo Monetario Internacional y la Unión Europea.[13]

Desde el 11 de septiembre de 2001, el gobierno de Estados Unidos reforzó dramáticamente las capacidades de sus servicios de inteligencia para recopilar e investigar la información de extranjeros y ciudadanos estadounidenses. Otro de los documentos altamente reveladores publicados por Snowden fue sobre el programa conocido con el nombre de PRISM. Este programa ejecutado por la NSA recoge datos electrónicos privados pertenecientes a los usuarios de los principales servicios de grandes empresas de Internet como Gmail, Facebook, Outlook, Microsoft, Apple y Yahoo, entre otros. Aunque el gobierno de Estados Unidos insiste en que sólo se le permite recoger datos cuando obtiene autorización por la FISA, en la práctica este programa también recoge datos de ciudadanos que no son sospechosos de conexión alguna con el terrorismo o cualquier delito. Además de éste, Snowden ventiló la existencia de otros programas que forman parte de operaciones encubiertas lideradas por la NSA, como por ejemplo: MUSCULAR, XKEYSCORE, BULLRUN y OLYMPIA.

Snowden también reveló lo que él denomina una arquitectura de la opresión refiriéndose a la infraestructura de espionaje de la NSA por medio de la cual se puede acceder directamente a las comunicaciones y los datos privados, y que constituyen una serie de programas de vigilancia ultra secretos que van más allá de lo que se ha dado a conocer públicamente. Su método de

[12] Te Guardian. Disponible en: http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1
[13] Orden del Tribunal de Vigilancia de Inteligencia Extranjera de Estados Unidos. Disponible en: http://s3.documentcloud.org/documents/709012/verizon.pdf

recolección de datos se resume en: detectar, conocer, recolectar, procesar, explotar y compartir todo. Por otro lado, junto con las revelaciones, Snowden escribió un documento, llamado *Manifiesto pro privacidad*[14], que contó con la firma y el apoyo de ciudadanos de todo el mundo. De ésta manera quedaba demostrado que existe apoyo global para la protección de la privacidad. Por todos estos acontecimientos puede decirse que en 2013 el mundo tomó conciencia de que la vigilancia digital por los gobiernos del mundo no conoce límites. Y, por tanto, la vigilancia masiva no es una práctica aislada. Las filtraciones de Edward Snowden develaron que existe la tecnología para vigilar a millones de usuarios de Internet. La NSA, y otras entidades similares, vigilan masivamente miles de comunicaciones bajo el argumento de la seguridad nacional y la lucha contra el terrorismo. La naturaleza digital de la información en Internet implica que todo lo que hacemos en línea deja una *huella,* es decir, rastros de navegación.

Es así, como la vigilancia indiscriminada ha roto numerosas leyes nacionales en los Estados Unidos. Internet comenzó su fase de expansión rápida en un contexto global marcado por la guerra contra el terror, con el aumento de las restricciones y violaciones de los Derechos Humanos, especialmente a la privacidad, y la intensificación de la vigilancia estatal. Los poderes expansivos concedidos a las agencias de inteligencia después de 11 de septiembre de 2001 violentan incluso la Constitución de Estados Unidos. Dos años después del éxito contra SOPA (Stop Online Piracy Act) y PIPA (Patriotic IP Act) en los Estados Unidos, la comunidad activista por una Internet libre y sin espionaje, se está posicionando para la próxima batalla: el respeto a los derechos en la *era digital*.

En definitiva, Snowden merece el mérito de abrir el debate sobre las restricciones de los poderes estatales para vigilar las comunicaciones de los ciudadanos y para almacenar sus datos, dentro de la sociedad civil. Pues el irrestricto respeto a la privacidad ajena en las comunicaciones persigue un claro objetivo de dominio hegemónico mundial. Partiendo de ello, en el marco de la 24ta. Sesión del Consejo de Derechos Humanos de las Naciones Unidas, diversas organizaciones de la sociedad civil encabezadas por la Fundación por las Fronteras Electrónicas (Electronic Frontier Foundation, EFF) manifestaron ante las naciones la urgente necesidad de cumplir y asegurar los Derechos Humanos y proteger a sus ciudadanos de los peligros que presenta la vigilancia digital masiva.

[14] Edward Snowden. *Manifiesto pro Privacidad.*
Disponible en: http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document Fecha de consulta: julio de 2014.

II. ¿Quién controla Internet?

A. La Gobernanza en Internet

En 2006 surge el Foro para la Gobernanza de Internet (IGF)[15], producto de un proceso abierto e inclusivo, y fue apoyado por la Asamblea General de las Naciones Unidas mediante una resolución[16] en la que reconoce la importancia del Foro para fomentar la sostenibilidad, la solidez, la seguridad, la estabilidad y el desarrollo de Internet, así como su papel en la creación de alianzas entre los diferentes actores, ya que en éste, la sociedad civil tiene la posibilidad de participar en igualdad de condiciones junto con el sector privado y el gobierno. Pese a que el Foro no tiene capacidad de decisión resulta ser un espacio de diálogo que legitima el modelo *multistakeholder* brindando la oportunidad de un encuentro libre entre todos los actores, y propicia el debate sobre temas de políticas públicas relacionadas con Internet.

Según el Foro, la gobernanza de Internet es el desarrollo y la aplicación de principios claramente definidos que propician la participación multisectorial igualitaria tanto en el sector público como privado, así como normas, reglas, procesos de toma de decisión y programas que regulan el uso de Internet.[17]

B. La soberanía digital

Con el advenimiento de la era digital se instalan sobre la mesa de debate nuevos conceptos como el de *soberanía digital*, el cual para 1998 se convierte en un tema de estudio. Con el fin de, entender qué es la soberanía digital, y cómo funciona, debemos hablar de soberanía política. La soberanía política se define en torno al poder, a la facultad que posee cada Estado de ejercer el poder sobre su sistema de gobierno, su territorio y su población. Es decir, debe comprenderse desde la máxima noción de Estado soberano, pues, éste es el poder de un Estado de no ser sometido por ningún otro. La soberanía digital hace referencia a ese mismo concepto de poder pero en el ciberespacio (entendido como un espacio virtual en Internet), y viene a romper con la lógica de la soberanía política ya que.se caracteriza por la ausencia de fronteras establecidas, en la cual Internet puede constituir y, de hecho, constituye, una seria amenaza a la capacidad del

15 Foro de Gobernanza en Internet. *Sesión inaugural del Foro de Gobernanza de Internet*. Disponible en: http://www.intgovforum.org/cms/documents/igf-meeting/igf-2006-athens/128-igf-2006-summary-final/file
16 Unión Internacional de Comunicaciones. *Resolución adoptada por la Asamblea General 60/252: Cumbre Mundial sobre la Sociedad de la Información*. Disponible en: http://www.itu.int/wtisd/res60-252.html
17 Foro de Gobernanza en Internet. *Sesión inaugural del Foro de Gobernanza de Internet*. Disponible en: http://www.intgovforum.org/cms/documents/igf-meeting/igf-2006-athens/128-igf-2006-summary-final/file

Estado soberano de controlar los acontecimientos políticos y sociales que tienen dentro de sus fronteras. Por tanto, la propagación de tecnologías de la información y de la comunicación a través de internet socava el poder soberano.[18]

Internet tiene reglas de gestión dictadas exclusivamente por Estados Unidos y, América Latina es el continente con las redes de telecomunicaciones más dependientes de éste país, ya que gran parte del tráfico en Internet pasa por servidores norteamericanos y un alto porcentaje de los contenidos digitales de Latinoamérica se encuentran alojados en Estados Unidos. La intervención responde a un ideal de soberanía similar al de gobiernos autocráticos, donde el soberano se ve amenazado por las nuevas formas de comunicación[19.] Por ello, es un error pensar que la intervención a las comunicaciones se desarrolla desde la base de un Estado democrático, ya que la intervención masiva a las comunicaciones va en contra de la soberanía digital.

En 2013, Julián Assange[20] denunció que internet ha sido ocupada militarmente por Estados Unidos y sus aliados para dominar a las sociedades atentando contra su soberanía nacional. Assange, también denunció el riesgo en que se encuentra la soberanía digital en Latinoamérica y el Caribe pues, como se menciona antes, gran parte del tráfico de sus comunicaciones transita a través de cables de fibra óptica que físicamente pasan por Estados Unidos, y esto se traduce en una grave amenaza a la privacidad.

C. Neutralidad en la Red

La Comisión Federal de Comunicaciones de Estados Unidos (FCC), creada desde 1934, considera que internet debe ser concebido como un bien público. Ésta Comisión defiende el concepto de neutralidad en Internet como un conjunto de reglas creadas para prevenir que los proveedores de los servicios de Internet realicen cambios en la velocidad para favorecer a algunos sitios o bloqueen el acceso a algunas páginas legales. En mayo de 2010, la FCC presentó a la Corte de Apelaciones para el Distrito de Columbia, Estados Unidos[21], una propuesta en la que define las reglas para la protección de la neutralidad en Internet en la cual se expresa que las

18 Aoki, Keith. "Multiple and overlapping sovereignty: liberalism, libertarian doctrine, national sovereignty, "global" intellectual property and Internet". *Indiana Journal of Global Legal Studies (April 1998)* 446.

19 Henry Perritt, "The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance". Indiana Journal of Global Legal Studies (April 1998). 431. Disponible en: http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1128&context=ijgls

20 Julian Assange, periodista australiano, programador y activista de Internet.

21 Corte de Apelaciones para el distrito de Columbia, Estados Unidos. "Verizon VS. FCC". Disponible en: http://www.cadc.uscourts.gov/internet/opinions.nsf/3AF8B4D938CDEEA685257C6000532062/$file/11-1355-1474943.pdf

empresas proveedores de servicios de Internet (ISP, por sus siglas en inglés) no deben bloquear sitios web o imponer límites en los usuarios.[22]

La idea de la neutralidad en Internet es que los proveedores deben tratar por igual a todos los datos que viajan a través de sus redes. Los principios básicos y las reglas[23] de neutralidad en la red que deberán seguir los grandes proveedores de Internet fueron aprobadas por el gobierno de Estados Unidos[24] en febrero de 2015[25]. Sin embargo, los proveedores aún están a tiempo de solicitar el aplazamiento de la aplicación de estas reglas.

Se debe tener en cuenta que la FCC no fue la única fuerza impulsora detrás de éstas reglas, hay que dar crédito también a la coalición entre organizaciones de sociedad civil, sectores no organizados de la sociedad y empresas privadas estadounidenses. Por otro lado, preocupa que la FCC haga referencia a la posibilidad de que Internet sea clasificada como un servicio de transmisión regulado estableciendo reglas de prohibición como la priorización de pago y bloqueo o filtrado de contenidos.[26] La priorización de pago es una alteración de la neutralidad de la red pues permite a los proveedores hacer una discriminación selectiva entre los datos que estén en tránsito de un sitio web a otro, es decir, ningún paquete de datos debería ser separado a una vía lenta por no pagar una cuota determinada, porque esto socava la igualdad de condiciones que es esencial para el crecimiento y desarrollo de internet libre.[27] Y, para garantizar la privacidad en internet, los proveedores de servicio no deben manejar los contenidos.

El objetivo de la neutralidad de la red es que todo lo que se transmita por la red se transmita de la misma forma, es decir, sin discriminar ni distinguir el contenido de los paquetes. La neutralidad de la red es fundamental para garantizar la pluralidad y diversidad del flujo informativo. Para ello, no debe haber discriminación, restricción, bloqueo o interferencia en la transmisión del tráfico de internet, a menos que sea estrictamente necesario y proporcional para preservar la integridad y seguridad de la red.[28] La neutralidad de la red es uno de los grandes principios sobre los que se

22 Federal Communications Commission. “Protecting and Promoting the Open Internet”. Disponible en: http://www.fcc.gov/document/protecting-and-promoting-open-internet-nprm
23 Federal Communications Commission. “FCC adopte, las Reglas fuerte y sostenible para la Protección de la Internet abierta” Disponible en: https://apps.fcc.gov/edocs_public/attachmatch/DOC-332260A1.pdf
24 The White House. “Net Neutrality”. Disponible en: https://www.whitehouse.gov/net-neutrality
25 Federal Communications Commission. “Open Internet”. Disponible en: http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0403/FCC-15-24A1.pdf
26 The Daily Dot. “Title II is the key to net neutrality“. Disponible en: http://www.dailydot.com/politics/what-is-title ii-net-neutrality-fcc/
27 Electronic Frontier Foundation. “Net Neutrality”. Disponible en: https://www.eff.org/es/issues/net-neutrality
28 Gobierno de la República de Brasil. “Ley No. 12.965”. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

ha construido Internet y supone aplicar a todos los datos que circulan por la red el mismo tratamiento, sin que haya prioridad ni jerarquía[29], e implica pues que en Internet nadie puede bloquear una conexión entre dos nodos[30.] Dicho de otra manera: la neutralidad en Internet contribuye a que no se viole el derecho a la privacidad y la intimidad, pues, el uso de cualquier técnica que intercepte o inspeccione el contenido de comunicaciones, es decir, el tráfico de datos en Internet, va en contra del derecho a la protección de datos[31] y del derecho de la privacidad.

Las consecuencias de la regulación de la red de un país, pueden sentirse en otro. En consecuencia, el bloqueo, filtrado o priorización de contenidos puede impactar a cualquier posible servidor o destinatario de esos contenidos. Esto es especialmente sensible a propósito de las redes en Estados Unidos: dado que varios de los servicios más importantes del mundo tienen servidores en su territorio, las condiciones de ese tránsito tienen consecuencias sobre el alcance de los contenidos requeridos o enviados.

La neutralidad de la red como un principio obligatorio ha comenzado su consagración en Latinoamérica. En 2010, Chile se convirtió en el primer país del mundo en proteger por ley el principio de la Neutralidad de la Red[32] garantizando la ausencia de restricciones de parte de los proveedores de servicios sobre los paquetes de datos. En específico, la ley establece que los proveedores no pueden arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet. No obstante, se acepta que puedan bloquear el acceso a determinados contenidos, aplicaciones o servicios a pedido y costo del usuario.[33] Actualmente, en Chile es posible apreciar algunos efectos positivos desde la aprobación de la ley, como la disminución de costos de conexión, incremento del número de usuarios y la introducción de mayor competitividad en el mercado de telecomunicaciones. Sin embargo, existen irregularidades en la fiscalización que la autoridad pública hace sobre la ley[34], pero marca un precedente.

29 Internautas. “Manifiesto por los Derechos Civiles y la Neutralidad en la Red”. Disponible en: *http://www.internautas.org/acciones/acto24052009/manifiesto.html*

30 Punto de conexión de varios elementos que coinciden en el mismo lugar. Ejemplo: En redes de computadoras cada una de las máquinas es un nodo, y si la red es Internet, cada servidor constituye también un nodo.

31 Organización de Estados Americanos. “Protección de Datos Personales”. Disponible en: http://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp

32 Subsecretaria de Comunicaciones de Chile. “Reglamento que regula las características de la neutralidad en la red de los servicios de acceso a internet”. Disponible en: http://www.subtel.gob.cl/images/stories/articles/subtel/asocfile/10d_0368.pdf

33 Reglamento que regula las características de la neutralidad en la red de los servicios de acceso a internet. (Chile: Subsecretaria de Comunicaciones, 2010). Artículo 24, H.

34 Digital Rights. “Una Evaluación de la Ley de Neutralidad de la Red en Chile”. Disponible en: http://www.digitalrightslac.net/es/una-evaluacion-de-la-ley-de-neutralidad-de-la-red-en-chile/

Por otro lado, Brasil ha dado un paso histórico con la elaboración y aprobación de la ley de marco civil que se aprobó en abril de 2014[35]. El objetivo de éste marco civil es garantizar la privacidad en la web y establecer pauta claras para la neutralidad en Internet. La iniciativa fue impulsada por la presidenta Dilma Rousseff, luego de que en 2013 Edward Snowden diera a conocer detalles sobre el espionaje de la Agencia de Seguridad Nacional de Estados Unidos hacia distintos dirigentes mundiales, incluyendo a la mandataria brasileña.[36] El marco civil promueve el respeto a los derechos civiles en el uso de internet en Brasil, y surge como producto de un largo debate promovido por la sociedad civil.

Sin embargo, a pesar de estos grandes pasos regionales en América Latina, la neutralidad de la red aún está en riesgo ante la aprobación de leyes como la Ley de Telecomunicaciones del Ecuador[37]. El gobierno de Ecuador considera la ley como una herramienta de política pública que promueve el desarrollo adecuado de las telecomunicaciones, bajo una visión orientada a fomentar el acceso universal a las Tecnologías de la Información y Comunicación. La ley garantiza el principio de neutralidad de la red, pero con ciertas irregularidades otorgando un fuerte control al presidente. Mientras que el Plan Nacional de Desarrollo 2014-2018 de Colombia[38], sostiene que la neutralidad de la red sigue estando a disposición del gobierno de turno. En Marzo de 2015, un grupo de organizaciones civiles envió una carta abierta al Gobierno y al Congreso para exigir el respeto a éste principio, argumentando que no se debe desconocer el deber estatal de proteger el derecho a la libertad de expresión y el derecho a la intimidad contemplados por numerosos instrumentos internacionales suscritos por Colombia[39].

De tal forma, para que Internet permanezca abierta y global, es imperativo que los Estados aborden las preocupaciones de seguridad de acuerdo con sus obligaciones internacionales en Derechos Humanos, en particular en lo que respecta a la libertad de expresión, la libertad de asociación y la privacidad[40]. Por tanto, es de suma importancia que se reconozca que la vigilancia

35 Gobierno de la República de Brasil. “Ley No. 12.965”. Dispnible en: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
36 The Guardian. “NSA acusado de espiar a la petrolera brasileña Petrobras”. Disponible en: http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras
37 Asamblea Nacional. “Ley Orgánica de Telecomunicaciones”. Disponible en: http://amchamgye.org.ec/images/NOTICIAS/Ley%20Org%C3%A1nica%20de%20Telecomunicaciones%20y%2 Servicios%20postales%20-%202011.pdf
38 Departamento Nacional de Planeación. “Bases Plan Nacional de Desarrollo 2014-2018”. Disponible en: https://colaboracion.dnp.gov.co/CDT/Prensa/Bases%20Plan%20Nacional%20de%20Desarrollo%202014 2018.pdf
39 Fundación para la Libertad de Prensa. “Carta abierta al Gobierno y a los Congresistas colombianos sobre la Neutralidad de Internet”. Disponible en: http://flip.org.co/es/content/carta abierta-al-gobierno-y-los-congresistas-colombianos-sobre-la-neutralidad-de-internet
40 Alto Comisionado de Derechos Humanos las Naciones. “Right to Privacy in the Digital”. Disponible en:http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en

masiva, y sistemática, es de por sí desproporcionada y no cumple con los estándares internacionales de los Derechos Humanos.

III. Tecnopolítica: la revolución 2.0

Internet, las redes sociales y los teléfonos móviles realzan la libertad humana de congregarse en torno a los temas sociales, políticos y económicos, construir asociaciones y redes, y convocarse para promover y defender los Derechos Humanos. Así como se demostró en las manifestaciones y protestas que tuvieron lugar en Oriente Medio y el Norte de África (2011); en las protestas contra las medidas de austeridad en Grecia (2010), España (2011) e Italia (2013); en las protestas englobadas con el nombre de Occupy; en las manifestaciones contra las leyes SOPA (Stop Online Piracy) y PIPA (Protect IP Act) en Estados Unidos; en las protestas estudiantiles en Canadá y Chile; y el movimiento ciudadano por la democratización de los medios de comunicación, la creación de un tercer debate presidencial y el rechazo a la supuesta imposición mediática en México. Por otro lado, las respuestas de los gobiernos al ejercicio de estos derechos se tradujeron en medidas represivas33 en Egipto, Libia y Siria, constituyendo este comportamiento una amenaza a la libertad de asociación y de reunión pacífica.

Es un hecho que con la aparición de plataformas como Twitter, Facebook y YouTube se han redefinido espacios de posicionamiento. Y, en este escenario, las Tecnologías de la Información y la Comunicación (TIC) juegan un papel de vital importancia en el nuevo contexto ideológico, político y cultural de la dictadura del pensamiento único, puesto que dentro de esta nueva lógica en la que, por ejemplo, las redes sociales constituyen una herramienta de resistencia virtual, se reduce la dependencia de los canales tradicionales de comunicación. Partiendo de éste punto, se conciben las bases de las nuevas formas de organización social que evolucionan al ritmo de los avances tecnológicos. De ésta manera, el ciberespacio se convierte en un centro de operaciones para los movimientos sociales donde se propone un espacio contra hegemónico con todas las sanas intenciones de romper el bloqueo informativo y distorsionante de los grandes medios de comunicación.

A. El acceso a internet; un derecho humano.

En 2011, la Asamblea General de las Naciones Unidas, en su informe para la promoción, protección y disfrute de los derechos humanos en Internet[41], declaró el acceso a internet como derecho humano fundamental altamente protegido, y exigió a los países miembros facilitar un servicio accesible a internet para la población. Violaciones a este derecho humano abarcan: el bloqueo a la web o filtrado de contenidos, la desconexión para evitar el acceso, los ciberataques, la falta de protección al derecho a la privacidad y la falta de protección de datos personales, entre otros.

El informe expone las tendencias y desafíos clave para el derecho de toda persona a buscar, recibir y difundir información, y compartir ideas, de todo tipo a través de internet. También, enfatiza la naturaleza única y transformadora de internet no sólo para que las personas puedan ejercer su derecho a la libertad de expresión, sino también como un facilitador de otros derechos, incluidos los derechos económicos, sociales y culturales, como el derecho a la educación y el derecho a participar en la vida cultural y gozar los beneficios del progreso científico y de sus aplicaciones, así como los derechos civiles y políticos, y también los derechos a la libertad de asociación y reunión para promover el progreso de la sociedad en su conjunto.[42]

Es importante remarcar que el Relator especial sobre el derecho a la libertad de reunión y asociación pacíficas reconoce ha reconocido que el "papel de Internet ha sido decisivo para facilitar la participación activa de la ciudadanía en la construcción de sociedades democráticas"[43]. Asimismo ha recomendado a los estados reconocer "la posibilidad de ejercer los derechos a la libertad de reunión y de asociación pacífica a través de las nuevas tecnologías, incluido el Internet"[44].

En noviembre de 2013, la Asamblea General de las Naciones Unidas, por medio del Relator especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, publicó una resolución sobre el *Derecho a la Privacidad en la Era Digital*[43], en la cual se reafirma que los derechos de las personas, incluido el derecho a la privacidad, deben ser debidamente protegidos en Internet. La Resolución especifica puntos como: a) el respeto y protección a la privacidad, incluso en el contexto de las comunicaciones digitales; b) la necesidad de adoptar medidas para poner fin a las violaciones de esos derechos y creen las condiciones

41 Relatoría Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. "Promoción, protección y disfrute de los derechos humanos en Internet " Disponible en: http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf
42 Relatoría Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. Disponible en: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
43 Resolución A/C.3/68/L.45/Rev.1

necesarias para impedirlas; y c) examinar los procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales.

Ésta resolución, hace referencia a un informe[44] previo del Relator Frank La Rue, en cuanto a las implicaciones de la vigilancia e interceptación extraterritoriales de las comunicaciones realizada por los Estados. El informe examina el impacto de los avances tecnológicos significativos en comunicaciones y pone de relieve la urgente necesidad de estudiar más a fondo las nuevas modalidades de vigilancia y de revisión de las leyes nacionales que regulan estas prácticas en consonancia con ´los estándares internacionales de Derechos Humanos, asimismo identifica los riesgos que los nuevos medios y modalidades de la vigilancia de las comunicaciones suponen para los Derechos Humanos, incluido el derecho a la privacidad y la libertad de opinión y de expresión.

No cabe duda, que la comunidad de activistas por el derecho a la privacidad, la libertad de expresión y por la libertad de Internet, le debe mucho al ex Relator Frank La Rue quien terminó su segundo mandato a mitad de 2014 y quien se posicionó, desde su relatoría, con un enérgico y contundente discurso por el derecho a la privacidad y a la libertad de expresión, se manifestó contra del intervencionismo de estado y de la criminalización a las formas legítimas de expresión. Es un ferviente activista por los derechos digitales que logró también borrar la barrera generacional, y se lo extraña, desde ésa trinchera de lucha.

[44] A/HRC/23/40

Bibliografía

Aoki, Keith. “Multiple and overlapping sovereignty: liberalism, libertarian doctrine, national sovereignty, "global" intellectual property and Internet”. Indiana Journal of Global Legal Studies (April 1998) 446.

Becker. “Outsiders: Studies in the Sociology of Deviance”. New York. New York The Free Press. 1963. Pp. 1-2, 162.
http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1128&context=ijgls

Electronic Frontier Foundation. “Amicus Brief of Experts in the History of Executive Surveillance”. Disponible en: https://www.eff.org/es/document/amicus-brief-experts-history-executive-surveillance

Electronic Frontier Foundation. “Net Neutrality”.
Disponible en: https://www.eff.org/es/issues/net-neutrality

Federal Communications Commission. “Open Internet”. Disponible en:

http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0403/FCC-15-24A1.pdf

Federal Communications Commission. “Protecting and Promoting the Open Internet”. Disponible en: http://www.fcc.gov/document/protecting-and-promoting-open-internet-nprm

Foro de Gobernanza en Internet. Sesión inaugural del Foro de Gobernanza de Internet. Disponible en: http://www.intgovforum.org/cms/documents/igf-meeting/igf-2006-athens/128-igf-2006-summary-final/file

Marx, Gary T.. “Surveillance and Society”. Thousand Oaks , California. Encyclopedia of Social Theory. 2005. Pp 817-822

Merton, Robert K.. “Anomie, Anomia and Social Interaction: Contexts of Deviant Behavior”. New York. New York The Free Press. 1964. P. 213.

Orwell, George. “1984”. Barcelona. Ediciones Destino. 2009.

Perritt, Henry, “The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance”. Indiana Journal of Global Legal Studies (April 1998). 431. Disponible en: The White House. “Net Neutrality”. Di
sponible en: https://www.whitehouse.gov/net-neutrality

Privacy International. “The Five Eyes”. Disponible en: https://www.privacyinternational.org/?q=node/51

Unión Internacional de Comunicaciones. Resolución adoptada por la Asamblea General 60/252: Cumbre Mundial sobre la Sociedad de la Información. Disponible en: http://www.itu.int/wtisd/res60-252.html

Palabras clave

Derechos humanos
Vigilancia
Privacidad
Libertad de expresión
Intervención
Soberanía
Neutralidad
Poder.

Key words

Human Rights
Surveillance
Privacy
Freedom of expression
Intervention
Sovereignty
Neutrality
Poverty