Construyendo una participación informada en torno a la Gobernanza de Internet

Miércoles, 5 de octubre de 2016

Antecedentes

El 15 de diciembre de 2015 la Asamblea General de Naciones Unidas adoptó la Resolución A/70/125, *"Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información*"[1], en cuya sección relacionada con el Foro de Gobernanza de Internet se destacan los siguientes elementos:

- Se reitera la definición de trabajo de gobernanza de internet, que la considera "el desarrollo y la aplicación, por parte de los gobiernos, el sector privado y la sociedad civil, en sus respectivos papeles, de principios, normas, reglas, procesos de toma de decisiones y programas compartidos que configuren la evolución y el uso de internet".
- Se reconoce que la gestión de internet como un recurso mundial incluye procesos multilaterales, transparentes, democráticos y de múltiples partes interesadas.
- Se reafirman los acuerdos de la Declaración de Principios de Ginebra en cuanto a que la gestión de internet abarca cuestiones técnicas y de política pública, y que debe considerar a todas las partes interesadas.
- Se reconoce la función del Foro para la Gobernanza de Internet como una plataforma de múltiples interesados para examinar cuestiones relacionadas con la gobernanza de internet, y se prorroga por otros diez años el mando actual del mismo.

De acuerdo con datos del Banco Mundial, en la actualidad alrededor de 4 mil millones de personas (el equivalente a dos tercios de la población total de los países en desarrollo), continúan sin acceso a internet a pesar de los esfuerzos que se han realizado para conectar a las personas alrededor del mundo, lo que demuestra que aún hay mucho camino que recorrer en cuestiones de política pública relacionadas con internet. Por esta razón, los foros de gobernanza de internet nacionales, regionales y el global cobran particular relevancia como plataformas para la discusión de temas que ayuden a que internet continúe desarrollándose en favor de las sociedades.

El Instituto Federal de Telecomunicaciones, en un esfuerzo por abonar a este mandato y con el fin de contribuir a elevar el interés e involucramiento de las partes interesadas en estos temas de cara al Foro Global de Gobernanza de Internet (6 al 9 de diciembre, Guadalajara, Jalisco), organiza el evento "Construyendo una participación informada en torno a la gobernanza de internet", en el que expertos provenientes de diversos sectores interesados abordarán algunos de los aspectos globales, regionales y locales de la gobernanza de internet con el objetivo de promover mayor participación en las

[1] El documento puede ser consultado en el siguiente link: http://goo.gl/U4BJsy

discusiones y hacer un llamado para fortalecer y mejorar las plataformas de diálogo, e incrementar su estabilidad y transparencia.

Programa

(Maestro de ceremonias: Coordinación General de Asuntos Internacionales)

8:30 – 9:00		Registro
9:00 – 9:30		**Apertura** Gabriel Contreras Saldívar Presidente IFT (confirmado)
9:30 – 10:00	SESIONES TEMÁTICAS	**Presentación sobre "Foro de Gobernanza de Internet en México (dic. 2016)"** Víctor Manuel Lagunes Soto Ruiz, Jefe de la Unidad de Innovación y Estrategia Tecnológica de la Oficina de la Presidencia de la República.
10:00 – 10:30		**Introducción a la gobernanza de internet para nuevos participantes** Manuel Haces. Gerente de Prospectiva y Regulación, NIC México (confirmado).
10:30 – 12:30		**Ciberseguridad** *Moderador:* *Alejandro Pisanty Baruch. Profesor de tiempo completo, Facultad de Química, UNAM (confirmado).* • Lina Ornelas. Jefa de políticas públicas y relaciones con gobierno, Google (confirmada). • Fernando Arredondo. Gerente de seguridad, NIC México (confirmado). • Julio Téllez Valdés. Investigador titular, Instituto de Investigaciones Jurídicas, UNAM (confirmado). • Eduardo Espina García. Director de seguridad, Mnemo (confirmado). • Pablo Corona. Vicepresidente de seguridad, AMIPCI (confirmado). • Nohemí González Vergara, Seguridad de datos personales, INAI (confirmada). • Paulina Gutiérrez, Article 19 (confirmada).
12:30 – 13:00		Descanso para café
13:00 – 14:30		**Impacto de los acuerdos comerciales y tratados de libre comercio en internet** *Moderadora:* *Cyntia Martínez Maldonado. Presidenta, AMIPCI (confirmada).* • Gabriela Cuevas Barrón. Presidenta de la Comisión de Relaciones Exteriores, Senado de la República (confirmada). • Juan Carlos Baker Pineda. Subsecretario de Comercio Exterior, SE (confirmado). • Mario Fromow Rangel, Comisionado del IFT (confirmado). • Fernando Portugal. Director divisional de relaciones internacionales, IMPI (confirmado). • Miguel Calderón Lelo de Larrea, Vicepresidente de la Comisión de Economía Digital de la International Chamber of Commerce (confirmado). • Olivia Andrea Mendoza Enríquez. Investigadora, INFOTEC (confirmada). • Erik Huesca Morales. Consejero, Consejo Consultivo del IFT (confirmado).
14:30 – 16:00		Comida
16:00–17:45		**Políticas públicas de accesibilidad y reducción de la brecha digital en internet** *Moderador:* *Luis Miguel Martínez Cervantes. Consejero, Consejo Consultivo del IFT (confirmado).* • Alfonso Hernandez Maya. Coordinador General de Política del Usuario, IFT (confirmado). • Tania Paola Cruz, Directora General de Servicios Digitales de la Unidad de Gobierno Digital, Secretaría de la Función Pública (confirmado).

		• Fernando Borjón. Director general, Organismo Promotor de Inversiones en Telecomunicaciones, SCT (confirmado). • Carlos Brito. Derechos Digitales (confirmado). • Carlos Casasús. Corporación universitaria para el desarrollo de internet (confirmado). • Ana Elena Fierro Ferráez. Investigadora, CIDE (confirmada). • Erick Huerta Velázquez. Consejero, Consejo Consultivo del IFT (confirmado). • Daniel Ríos, Director de política, AT&T (por confirmar).
17:45 – 18:15		**Sesión informativa. Transición de las funciones de IANA: implicaciones para la gobernanza de internet** *León Felipe Sánchez. Co-Presiente del CCWG (confirmado)*.
18:15 – 18:30		**Conclusiones y clausura del foro** *Juan Carlos Hernández, Coordinador general de asuntos internacionales, IFT.*

Contenidos del encuentro

1. Introducción a la gobernanza de internet para nuevos participantes

Esta sesión de introducción está destinada tanto a los recién llegados al tema de gobernanza de internet como a quienes ya están involucrados y desean obtener una visión más integral del tema. Se pretende lograr una sesión interactiva, educativa e inclusiva, que genere un acercamiento entre los nuevos participantes y los expertos en temas de gobernanza de internet para propiciar el diálogo entre ellos. Algunos detonadores de la conversación podrían ser:

- ¿Qué es la gobernanza de internet? ¿Cómo nace?
- ¿Qué es el Foro de Gobernanza de Internet global y sus antecedentes?
- ¿Quiénes son los actores participantes?
- El modelo de múltiples partes interesadas (*multistakeholder*) y el papel de cada actor interesado.

2. Ciberseguridad

El objetivo fundamental del panel es debatir las amenazas relativas a la vigilancia, privacidad, resiliencia y seguridad asociadas a la creciente digitalización, que ha provocado que dichos riesgos se hayan vuelto cada vez más complejos, sobre todo para los datos que circulan por las infraestructuras de internet, así como discutir las respuestas legales en torno a estas circunstancias. El panel busca fomentar, igualmente, la discusión en torno a la seguridad de la infraestructura y la resiliencia de la red, además de abordar temas como la estabilidad de la red, los ataques informáticos, la cultura de la ciberseguridad y la localización geográfica de la infraestructura, entre otros.

El Informe sobre Ciberseguridad 2016[2], publicado por el Banco Interamericano de Desarrollo (BID), la Organización de Estados Americanos (OEA), y el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la Universidad de Oxford, señala en México es necesario crear mecanismos para enfrentar los desafíos de la seguridad cibernética, sobre todo en lo que se refiere al fortalecimiento de la cooperación internacional para la protección del ciberespacio, el intercambio de información entre organismos, y la cooperación para la capacitación de los equipos de respuesta a incidentes de seguridad cibernética.

El mismo informe indica que el gobierno de México trabaja en la elaboración de una estrategia nacional de seguridad cibernética, en línea con una política que hace responsbles a las fuerzas armadas de la defensa cibernética. Además, el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX) es un parte del Foro de Equipos de Seguridad y de Respuesta a Incidentes (FIRST) y sigue un protocolo de colaboración con otras entidades gubernamentales. Según el mencionado informe, una división de la Policía Federal investiga los delitos cibernéticos nacionales y trabaja en estrecha colaboración con

[2] El Informe puede ser consultado en: http://goo.gl/3mVlbE

el CERT-MX. No obstante lo anterior, nuestro país se encuentra aún desarrollando una legislación integral sobre delincuencia cibernética, lo que dificulta el enjuiciamiento de los delitos cibernéticos a través de la legislación y regulación vigente en la materia, como el Código Penal Federal y la Ley de firmas electrónicas avanzadas.

La Unión Internacional de Telecomunicaciones (UIT) ha establecido un índice de ciberseguridad[3i], que representa una medida del nivel de desarrollo de la ciberseguridad de cada país. Este indicador pretende servir de estímulo para que los países intensifiquen sus esfuerzos en la materia, desde la perspectiva de contribuir al fomento de una cultura mundial de ciberseguridad, así como a su integración como elemento fundamental de las tecnologías de la información y la comunicación.

México está clasificado a nivel mundial en la posición 18, con un índice de 0.324. Ante estas cifras, los diversos *stakeholders* deben sostener un diálogo que diseñe un esfuerzo para informar a la sociedad mexicana de los problemas de seguridad cibernética. El perfil de México reporta lo siguiente:

- Medidas legales. La legislación específica sobre la ciberdelincuencia en México se encuentra en el Código Penal Federal. Su cumplimiento se ha dado a través de la Ley de firmas electrónicas avanzadas.
- Medidas técnicas. México tiene un *National Computer Incident Response Team* (CIRT) reconocido oficialmente como Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX).
- Medidas de estandarización. La norma ISO 207001 para un sistema de gestión de seguridad de la información es el marco reconocido a nivel nacional para la aplicación de normas de seguridad cibernética reconocidas internacionalmente. Su cumplimiento requiere de todas las instituciones gubernamentales clave para su efectiva ejecución. En México no existe un marco para la certificación y la acreditación de los organismos nacionales y del sector público con respecto a seguridad cibernética.
- Medidas en las organizaciones. El Comité de Seguridad de la Información Especializada (CESI) fe creado para desarrollar una estrategia nacional de seguridad de la información (ENSI), cuya finalidad es guíar las acciones de las entidades del gobierno federal destinadas a prevenir, identificar, neutralizar o contrarrestar los riesgos y las amenazas a la seguridad de la información. De acuerdo con la UIT, no hay una hoja de ruta nacional para la seguridad cibernética. La Policía Federal es la encargada de las estrategias nacionales de seguridad cibernética, de la política y el plan de trabajo de los organismos respectivos. No hay información comparativa nacional.
- Creación de capacidades. No hay proyectos o programas de investigación o desarrollo de las normas de seguridad cibernética, mejores prácticas ni directrices.

[3] El índice puede ser consultado en: http://goo.gl/2BAKp6

- El personal de la División Científica ha recibido formación especializada del sistema de desarrollo de la policía de México, así como de países como Colombia, Estados Unidos, Holanda y Japón. Los esfuerzos dirigidos por el gobierno para promover una mayor conciencia de seguridad cibernética han incluido la organización de varias conferencias para instituciones públicas, privadas y educativas.
- Referente a la certificación profesional, México no tiene un censo confiable de los profesionales del sector público certificados internacionalmente en programas de seguridad cibernética. Tampoco se cuenta con ninguna agencia gubernamental o del sector público certificada bajo normas reconocidas de seguridad cibernética a nivel internacional.
- En cuanto a la cooperación entre Estados, no hay información acerca de algún marco para compartir activos de seguridad cibernética con otra nación. México ha reconocido oficialmente los programas nacionales o sectoriales específicos para el intercambio de activos dentro de la ciberseguridad en el sector público a través de las autoridades del CESI, quienes también han desarrollado un protocolo de colaboración entre CERT-MX y otras dependencias del gobierno para abordar y responder a incidentes cibernéticos.
- CERT-MX también se comunica y colabora directamente con instituciones privadas.
- En referencia a la cooperación internacional, para facilitar la participación en plataformas regionales e internacionales de seguridad cibernética México es miembro de FIRST y OAS/CICTE.
- Protección infantil en línea. La legislación específica sobre protección de la infancia en línea ha sido promulgada a través de los siguientes instrumentos:
    - Ley Para la Protección de los Niños y Adolescentes (sin relación directa con internet).
    - México se ha adherido, sin declaraciones o reservas, a los artículos 16, 17 (e) y 34 (c) de la Convención sobre los Derechos del Niño.
    - México se ha adherido, sin declaraciones o reservas, a los artículos 2 y 3 del Protocolo Facultativo de la Convención sobre los Derechos del Niño, relativos a la venta de niños, la prostitución y la pornografía infantil.
    - El Consejo Nacional de Seguridad Pública ha emitido un documento a partir de un taller de cibercrimen que contiene información sobre las ciberamenazas. El Consejo Nacional de México trabaja en la seguridad de internet y da a conocer información sobre la seguridad para niños en internet. Existen una línea telefónica, un correo electrónico y una página web para canalizar quejas y denuncias.

El Foro Económico Mundial en su Informe de Riesgos Globales 2016[4], analiza las crisis tecnológicas y su relación con la seguridad de forma sistemática, y concluye que los dos riesgos más interconectados en 2016 son la profunda inestabilidad social y el desempleo estructural o subempleo, y los ciberataques. Algunos detonadores del diálogo en este panel podrían ser:

- ¿Cómo preservar el carácter libre, seguro y abierto de internet?
- ¿Qué políticas públicas que se necesitan desarrollar para garantizar la ciberseguridad sin perjuicio de los derechos humanos?
- ¿Qué participación deben tener los diferentes ccTLD frente a incidentes de ciberseguridad?

3. Impacto de los acuerdos comerciales y tratados de libre comercio en internet

En la actualidad un número creciente de cuestiones relacionadas a la ciberseguridad, tales como la resolución de nombres de dominio, el acceso a datos, el uso de los estándares de encriptación y mandatos de divulgación de código fuente, así como la información y flujos transfronterizos están siendo tratados multilateralmente en acuerdos comerciales tales como el Tratado de Asociación Trans-Pacífico (TPP), el Acuerdo de Comercio de Servicios (TISA), y la Alianza del Pacífico, entre otros.

Durante el mes de junio, en su informe titulado "*One Internet*"[5] la Comisión Mundial sobre el Gobierno de Internet escribió:

> *En términos de impacto en el mundo real, los acuerdos de libre comercio bilaterales y multilaterales pueden afectar significativamente la gestión de internet. Muchos, como el Acuerdo de Asociación Transpacífico, abordan específicamente los temas importantes tales como la localización de datos, la encriptación, la censura y la transparencia, temas que son generalmente considerados como parte del ecosistema de gobernanza de internet; Sin embargo, son temas que se negocian exclusivamente por los gobiernos.*

Sin embargo, la Organización Mundial de la Propiedad Intelectual también ha declarado que los tratados con impacto en internet buscan "mantener un equilibrio justo de intereses entre los titulares de los derechos y los consumidores".

Las negociaciones comerciales sobre estos temas están separadas de las discusiones más amplias de múltiples partes interesadas de esos mismos temas, y no se llevan a cabo mediante un proceso transparente o de múltiples partes interesadas. En particular, porque los Ministerios de Comercio nacional y los negociadores comerciales no perciben que estos puntos son cuestiones de Gobernanza de internet, sino como cuestiones comerciales.

[4] El Informe puede ser consultado en el siguiente enlace: http://goo.gl/GGa8vT
[5] El Informe puede ser consultado en el siguiente enlace: http://goo.gl/rpwGUV

Esto ha generado un gran debate en el seno de la comunidad de gobernanza de internet dado que, al no existir un verdadero dialogo *multistekeholder,* ha aumentado la preocupación de que la nueva generación de tratados comerciales implique una afectación de los derechos de los usuarios de internet, especialmente en lo que se refiere a la privacidad y la libertad de expresión e información.

Ante lo anterior, el objetivo de este panel es reflexionar sobre la necesidad de llevar a cabo un debate más amplio sobre la aplicación del modelo *multistakeholder* de la gobernanza de internet en las cuestiones comerciales**.**

Algunos puntos generadores de debate podrían ser:

- Los premios Nobel de economía Paul Krugman y Joseph Stiglitz han manifestado estar en contra del TPP argumentando que es imposible que beneficie a la población dado que establece leyes y condiciones que se traducen en barreras comerciales entre los miembros. ¿Qué se puede decir de los resultados benéficos a la población para contradecir esta afirmación?
- ¿Cuál es la relación entre los acuerdos comerciales y tratados de libre comercio y la propiedad intelectual en internet?
- ¿Cuál sería una medida para lograr un equilibrio entre los incentivos a creadores y el acceso social al conocimiento y cultura*,* la duración de los derechos de autor y la forma en que esta protección se hace cumplir en los acuerdos de internet?
- Las normativas de derecho de autor se están tomando en el marco de acuerdos comerciales que se discuten muchas veces de manera cerrada. ¿Cómo se puede asegurar la participación de sectores como la academia o la sociedad civil en dichas discusiones?
- ¿Consideran que para lograr una adecuada regulación en torno a los equilibrios, la discusión normativa debe abrirse más a temas comerciales?

Políticas públicas de accesibilidad y reducción de la brecha digital en internet

La Agenda 2030 para el Desarrollo Sostenible de las Naciones Unidas reconoce las grandes posibilidades que encierran las tecnologías de la información y comunicación y exhorta a que se aumente significativamente el acceso a ellas, que ha de aportar una contribución decisiva en apoyo a la aplicación de todos los objetivos de desarrollo sostenible (ODS).

Sin embargo, de acuerdo con el documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información, hasta 2015 sólo alrededor del 43% de la población mundial tenía acceso a internet, únicamente el 41% de las mujeres estaba conectado, y aproximandamente el 80% de los contenidos en línea estaba disponible en sólo uno de diez idiomas, por no hablar de la situación de desventaja que, con respecto al acceso a estas tecnologías, experimientan las personas con discapacidad. Así

pues, los ODS hacen un gran énfasis en el tema de accesibilidad como una prioridad para el desarrollo, y destacan la importancia de eliminar las disparidades de género, garantizar el acceso en condiciones de igualdad para las personas vulnerables, las personas con discapacidad, las mujeres, los pueblos indígenas, los niños y adolescentes.

Considerando lo anterior, el objetivo del panel es identificar las mejores prácticas que han permitido promover la inclusión y el acceso de todas las personas a las tecnologías de la información y comunicación, principalmente internet, así como, identificar el papel que juegan los diferentes *stakeholders* en la promoción de la accesibilidad para cumplir con las metas de los ODS. De igual manera, se buscará identificar los retos y desafíos en la generación de políticas públicas para incrementar la accesibilidad y reducción de la brecha digital en internet, con especial hincapié en el acceso equitativo y asequible, la promoción de una industrialización inclusiva y sostenible, el mejoramiento de la infraestructura mediante la adopción de tecnologías y procesos industriales limpios y ambientalmente racionales. Finalmente, se buscará identificar las medidas y estrategias que permitan aumentar considerablemente el acceso a las tecnologías de la información y la comunicación, así como disminuir la brecha digital que existe para las mujeres y niñas, las personas con discapacidad, y otros grupos vulnerables.

Algunos puntos adicionales a discutir podrían ser la cuantificación de la brecha digital y de las oportunidades existentes; las acciones de México en torno al seguimiento a la Reforma de Telecomunicaciones; la oferta disponible de acceso a Internet y nuevas opciones de conectividad; la creación de competencias digitales; la inclusión, indigenismo y equidad de género en el internet mexicano.

Algunos detonadores del diálogo en este panel podrían ser:

- ¿Qué temas de inclusión, más allá del acceso deben ser adoptados en nuestro entorno para aportar a una sociedad justa e incluyente?
- ¿Qué políticas públicas han sido implementadas por México para la reducción de la brecha digital?
- ¿Desde el punto de vista de cada *stakeholder*, qué hace falta para cerrar la brecha digital?
- ¿Cuáles son las principales prioridades de la región para fomentar la inclusión digital y fomento de la accesibilidad?

Transición de las funciones de IANA: implicaciones para la gobernanza de internet

El 14 de marzo de 2014, la Administración Nacional de Telecomunicaciones e Información de Estados Unidos (NTIA) anunció su intención de transmitir la custodia de las funciones de la Autoridad de Números Asignados de Internet (IANA) a la comunidad global *multistakeholder*. Posteriormente, el 10 de marzo de 2016, la Junta Directiva de ICANN presentó ante la NTIA la propuesta final de transición

de la custodia de la IANA y las “Recomendaciones para mejorar la responsabilidad de ICANN”, como resultado de un proceso de debate global e inclusivo entre gobiernos, sector privado, expertos técnicos, investigadores, sector académico, sociedad civil y usuarios finales.

De acuerdo con lo establecido por la NTIA, la propuesta debía cumplir con los siguientes principios: apoyar y mejorar el modelo *multistakeholder,* mantener la seguridad, estabilidad y resiliencia del sistema de nombres de dominio y de internet, satisfacer las necesidades y expectativas de los clientes y socios de los servicios de IANA, mantener la apertura de internet y que ninguna organización intergubernamental o una organización dirigida por un gobierno remplazara el papel que hasta ese momento ejercía la Administración.

Después de su revisión y evaluación, la NTIA concluyó que la propuesta presentada cumplía con todos los criterios previamente establecidos. De esta forma, el 9 de junio de 2016 la NTIA solicitó que ICANN presentará un informe sobre el estado de planificación e implementación. El 12 de agosto dicho reporte en donde indicó que todas las tareas requeridas para la transición estarían completadas para el 30 de septiembre. Finalmente, la NTIA informó que permitiría que el contrato de las funciones de IANA expirara el 1 de octubre del presente año. Por lo anterior, se considera pertinente una presentación general sobre el proceso que se llevó a cabo para la formulación de la propuesta de transición, los futuros pasos a seguir y las implicaciones que este proceso tendrá tanto para internet como para el modelo *multistakeholder* en la gobernanza de internet.