



Grupo de Expertos de Gobernanza

Proyecto Fundación Telefónica - Universidad Politécnica de Madrid

Sostenibilidad y Gobernanza de Internet: Propuesta de Temas para el Debate

Contribución a la IGF Conference Athens 2006

31 de julio de 2006

AUTORES:

Grupo de Expertos de Gobernanza

(Coordinador: Dr. Jorge Pérez)

CONTACTO

Dr. Sergio Ramos (coordinador adjunto)

e-mail: sramos@gtic.ssr.upm.es

Tel/Fax: +34 91 336 73 20

Móvil: +34 647 77 62 50

DIRECCIÓN

ETSI Telecomunicación – Universidad Politécnica de Madrid

Despacho C-431

28040 Madrid

España

ÍNDICE

INTRODUCCIÓN	3
ANÁLISIS INICIAL EN EL CONTEXTO DE LA IGF CONFERENCE ATHENS 2006: GOBERNANZA Y SOSTENIBILIDAD	5
PROPUESTAS PARA EL DEBATE SOBRE SOSTENIBILIDAD Y GOBERNANZA	8
NEUTRALIDAD DE RED.....	8
<i>Colectivos y posiciones</i>	9
<i>Temas de estudio</i>	10
SEGURIDAD, PRIVACIDAD Y CONFIANZA EN INTERNET.....	11
<i>Colectivos y posiciones</i>	12
<i>Temas de estudio</i>	15
BRECHA DIGITAL.....	16
<i>Colectivos y posiciones</i>	17
<i>Temas de estudio</i>	18
CONCLUSIONES	19
REFERENCIAS	20

INTRODUCCIÓN

La gestión y control de Internet es una cuestión que ha suscitado un amplio debate en el contexto internacional desde que la Red se convirtió en uno de los fenómenos económicos, sociales y políticos más importantes de los últimos años.

Ante el papel que las TIC desempeñan como uno de los pilares de la Sociedad de la Información, donde Internet es el elemento clave, y siendo asumido que el empleo de las TIC promueve el desarrollo y la mejora de las prácticas e interacciones sociales en relación a las infraestructuras, las transacciones y los intercambios de información a nivel internacional, surge un debate en el que aparece la necesidad de determinar los márgenes de autonomía relativos a las diferentes naciones y el nivel de participación de los diferentes agentes, pero no sólo en lo que a la gestión de los recursos técnicos de Internet se refiere, sino también a otras cuestiones como por ejemplo el reparto de responsabilidades para sufragar y corregir la brecha digital entre regiones ricas y pobres, la seguridad en Internet y otras redes de comunicaciones, la piratería digital o la distribución ilegal de contenidos multimedia.

Se habla por tanto de un nuevo paradigma regulador conocido como gobernanza de Internet, que en la pasada Cumbre Mundial de la Sociedad de la Información celebrada en Túnez en noviembre de 2005, se definió del siguiente modo:

“La gobernanza de Internet es el desarrollo y la aplicación por los gobiernos, el sector privado, y la sociedad civil, en las funciones que les competen respectivamente, de principios, normas, reglas, procedimientos de adopción de decisiones y programas comunes que configuran la evolución y utilización de Internet”

Entre las conclusiones de esta Cumbre cabe destacar el consenso alcanzado por extender la participación de todos los colectivos implicados en el desarrollo de Internet en el proceso de gobernanza iniciado, con el objetivo de avanzar en una dirección común basada en el diálogo, así como la colaboración con la comunidad académica y científica en la materia. Fruto de este acuerdo, Naciones Unidas¹ impulsó la creación del Internet Governance Forum, que celebrará su primera conferencia en Atenas en octubre de 2006².

A su vez se reconoció la necesidad de que cada nación debía diseñar sus propias políticas públicas atendiendo a criterios de identidad nacional y territorial en lo que se refiere a cultura, idioma y respeto a las libertades de cada individuo, siempre en sintonía con los convenios y acuerdos internacionales.

Es en este contexto y gracias al impulso de la Fundación Telefónica y al acuerdo de colaboración alcanzado con la Universidad Politécnica de Madrid, se ha constituido recientemente en España un Grupo de Expertos de Gobernanza con el objetivo de

¹ Cabe destacar las palabras del Secretario General de Naciones Unidas, Kofi Annan, al respecto: “...But I think you also all acknowledge the need for more international participation in discussions of Internet governance issues. The question is how to achieve this. So let those discussions continue...”

² Ver <http://www.igfgreece2006.gr/>

identificar el papel del sector TIC español y su Administración pública, las organizaciones de I+D y la sociedad civil en el desarrollo de Internet y de su gobierno en España y Latinoamérica. En definitiva se trata de poner de manifiesto la relevancia de esta cuestión para España y la necesidad de abordarlo desde el diálogo entre todos los estamentos y colectivos interesados.

Este Grupo nace con la vocación de constituirse en un foro de opinión y debate que aporte conocimiento en favor de la evolución y desarrollo de Internet y otras redes del conocimiento, participando e influyendo en los foros de decisión nacionales e internacionales sobre la gobernanza. El Grupo está integrado por profesionales que provienen de diferentes ámbitos curriculares, pero que en todos los casos desarrollan su actividad profesional, de forma directa o indirecta, dentro del sector de las telecomunicaciones, Internet y la Sociedad de la Información, y en el ámbito de las políticas públicas y sociales. De este modo se pretende que los trabajos llevados a cabo por el grupo integren las diferentes perspectivas de los participantes, ofreciendo una visión integradora y de conjunto de los temas tratados.

Así el presente documento es una aportación a la conferencia del Internet Governance Forum que se celebrará en Atenas en octubre de 2006, con el fin de participar en el debate planteado y promover cuestiones adicionales que desde el Grupo se consideran de especial interés y relevancia para el desarrollo de la gobernanza de Internet y otras redes del conocimiento.

ANÁLISIS INICIAL EN EL CONTEXTO DE LA IGF CONFERENCE ATHENS 2006: GOBERNANZA Y SOSTENIBILIDAD

Para elaborar esta contribución como aportación a la conferencia de Atenas se ha realizado una primera valoración del grado de coincidencia que diferentes colectivos pueden tener en lo que a intereses particulares sobre Internet y su desarrollo se refiere, particularizado al contexto español, de manera que se puedan extraer un conjunto de temas horizontales que faciliten la participación de todos los colectivos implicados en la gobernanza de Internet.

En la siguiente tabla se recoge una primera lista de agentes españoles junto con una valoración del interés que a priori pueden despertar para cada uno de ellos las diferentes cuestiones genéricas que articularán la conferencia del Internet Governance Forum en Atenas. A estas cuestiones (**apertura, seguridad, diversidad, acceso**) se les ha añadido una más que consideramos de vital importancia para incluir en el debate (tal y como se presenta en sucesivos apartados) la **sostenibilidad**:

- **Apertura.** Por apertura entendemos la cualidad de Internet como vehículo para la participación democrática, es decir, como lugar abierto a todo y a todos en el que a priori no existe control ni censura.
- **Seguridad.** Por seguridad denominamos al atributo básico del intercambio y uso de la información a través de Internet y sus implicaciones a nivel económico (p.e., comercio electrónico), político (p.e., protección de derechos de autor, propiedad intelectual, cibercrimen) y social (p.e., protección de consumidores y usuarios).
- **Diversidad.** La diversidad está directamente ligada al concepto de apertura, ya que podemos considerarla en lo que al ámbito de Internet se refiere como sinónimo de pluralidad, quedando patente la necesidad por el respeto a la opinión de todos y la igualdad entre colectivos, particularmente dando cabida a las minorías y los colectivos locales.
- **Acceso.** El acceso representa la capacidad de estar conectado, por cualquier medio y en cualquier lugar, a Internet.

Como se puede extraer de la siguiente tabla, es posible afirmar que desde un punto de vista general todas aquellas cuestiones ligadas con la seguridad y el acceso son prioritarias para la casi totalidad de los agentes españoles. Por su parte tanto apertura como diversidad parecen quedar en un segundo plano, siendo no obstante de gran relevancia para el colectivo público y la sociedad civil.

Estas cuestiones son evidentemente de vital importancia pero ninguna de ellas contempla un factor de gran relevancia a la hora de impulsar medidas concretas o adoptar una determinada posición. Nos referimos a las implicaciones económicas de cualquier acción, lo que hemos denominado **sostenibilidad**.

Tras analizar la evolución del debate de la gobernanza en el ámbito de la Cumbre Mundial de la Sociedad de la Información, así como otras iniciativas internacionales sobre la materia, desde el Grupo de Expertos de Gobernanza se observa que generalmente no se consideran las implicaciones económicas de las propuestas

planteadas, dejándose el análisis de la viabilidad y sostenibilidad económica al margen del debate de la gobernanza. Por ello creemos que sería muy interesante incluir esta cuestión en el marco de la conferencia del IGF de Atenas y articularla en torno a temas concretos que conciernen a todos los colectivos alrededor de Internet.

Por este motivo la tabla siguiente también recoge el interés o preocupación que los diferentes colectivos pueden tener a priori por buscar vías de diálogo o posiciones que fomenten la sostenibilidad de cualquier medida. Este interés quedaría particularmente representado por el sector público y parte del privado (operadores principalmente) seguido de las instituciones de I+D (que habitualmente introducen conceptos como viabilidad económica y sostenibilidad de los resultados que son fruto del proceso de I+D).

COLECTIVO	AGENTES	APERTURA	SEGURIDAD	DIVERSIDAD	ACCESO	SOSTENIBILIDAD
SECTOR PÚBLICO	SETSI	XXX	XXX	XXX	XXX	XXX
	CMT	X	XX	X	XXX	XX
	Red.es	XXX	XXX	XXX	XXX	XXX
	Operadores (Telefónica, Vodafone, Jazztel, Ono, ...)	X	XXX	X	XXX	XXX
SECTOR PRIVADO	ISP (Google, Yahoo, ...)	XX	XXX	XX	XXX	X
	Fabricantes (Lucent-Alcatel, Nokia, Ericsson, Siemens, ...)	X	XXX	X	XXX	XX
	AETIC	XX	XXX	XX	XXX	XXX
I+D	Universidades	XXX	XXX	XXX	XXX	XXX
	Fundaciones	XXX	XXX	XXX	XXX	XXX
	Institutos	XXX	XXX	XXX	XXX	XXX
ONGs	Asociaciones de usuarios	XXX	XXX	XXX	XX	X
	Asociaciones de consumidores	XXX	XXX	XXX	XX	X

Tabla 1. Mapa de agentes en España

Fuente: Elaboración propia

X – bajo; XX – medio; XXX – alto

PROPUESTAS PARA EL DEBATE SOBRE SOSTENIBILIDAD Y GOBERNANZA

Dada la necesidad de abordar cuestiones que en nuestra opinión conduzcan a propuestas y resultados donde se contemple la sostenibilidad de las mismas como un elemento central en el proceso de gobernanza de cualquier aspecto de Internet, los temas inicialmente seleccionados responden a dos criterios básicos: horizontalidad (es decir, temas en los que la participación de todos los colectivos es fundamental ya que todos están directamente implicados) y sostenibilidad.

Con este planteamiento se han seleccionado tres temas horizontales que se proponen para incluir en el debate de la conferencia de Atenas y para los que dar respuesta a la sostenibilidad económica de los mismos es un elemento esencial:

- Neutralidad de red.
- Seguridad, privacidad y confianza en Internet.
- Brecha digital.

NEUTRALIDAD DE RED

Una primera definición de neutralidad de red se refiere al principio por el cual se establece que todo el tráfico que circula por Internet debe ser tratado en condiciones de igualdad, al margen de cuál sea el contenido y quienes sean emisor y receptor.

La importancia del debate sobre neutralidad radica en el planteamiento de dos concepciones diferentes sobre la estructura de Internet: por un lado, si debe permanecer neutral como ha ocurrido desde sus inicios o, por el contrario, debe privatizarse para poder hacer frente a las nuevas exigencias, debidas precisamente a su desarrollo social, tecnológico y comercial.

Internet desde sus comienzos fue concebida como una red con estructura neutral y un diseño basado en la arquitectura extremo a extremo, de forma que fuera una red sencilla en su utilización y que permitiera a cualquiera el desarrollo de aplicaciones con la única condición de utilizar el protocolo IP.

La neutralidad de red garantiza que todos los flujos de información sean tratados en condiciones de igualdad y no sufran discriminación alguna, por tanto, una red que curse tráfico bajo estas premisas no sería capaz de ejercer ningún tipo de censura o presión anticompetitiva sobre la información que transporta³. Esto aseguraría la libre expresión por parte de todos los usuarios de Internet debido a que no existiría ninguna censura o modelado del tráfico por parte de ningún organismo o empresa, y sería directamente el usuario el que accediera a la información por su propia voluntad. Por consiguiente se le considera un esquema muy adecuado para mantener el derecho a la libertad de información y de expresión de todos los internautas. No obstante, esto no quiere decir que una arquitectura de red no neutral tenga que ser forzosamente discriminatoria.

³ Ver (Wu, 2003)

Precisamente lo que inicialmente ha sido clave en el desarrollo de Internet (su neutralidad) en estos momentos se ve cuestionado, ya que existen múltiples dudas sobre si podrá hacer o no frente a los desafíos presentes y futuros⁴:

- Proporcionar seguridad frente a conductas no amistosas.
- Garantizar la calidad de las nuevas aplicaciones.

El problema reside en que satisfacer estas demandas impuestas por la nueva realidad de Internet exige penetrar en la propia red e introducir una cierta inteligencia que pueda controlar los paquetes que están circulando, sea deteniéndolos (por razones de seguridad) o priorizándolos (por razones de negocio).

COLECTIVOS Y POSICIONES

Al igual que en todos los aspectos relacionados con la gobernanza, existen también diferentes opiniones acerca de la conveniencia de adoptar una arquitectura de Internet que respete la neutralidad como principio legal, y no como un estándar de facto como viene sucediendo.

Desde un punto de vista general, el debate actual se centra en el sector privado, con claras posiciones antagonistas entre los proveedores de servicios de Internet y los operadores de telecomunicaciones. Sin embargo, para el desarrollo de este proyecto la neutralidad de red debe ser entendida como una cuestión que afecta a todos los colectivos y que por su carácter global debería tratarse como tema prioritario en el modelo de gobernanza de Internet que hemos descrito.

A continuación presentamos las principales posiciones de los colectivos de agentes implicados en la gobernanza de Internet sobre la neutralidad de red:

- **Sector público.** Conceptualmente no existen argumentos claros para tomar una u otra posición ya que teóricamente cualquiera de las opciones propuestas podría en principio satisfacer los objetivos de interés público. Integrar la realidad expansiva que es Internet en un marco regulador que no la anticipó en su momento y se ve desbordado por el dinamismo tecnológico y de los mercados constituye una preocupación constante de las agencias reguladoras en la mayoría de países, en particular la Federal Communications Commission⁵ (FCC) en Estados Unidos. De hecho, en el centro del debate está la propuesta de que la FCC dé carácter normativo al principio de *net neutrality*, hasta ahora sólo una característica establecida de facto para Internet⁶.

⁴ Ver (Comín, 2006)

⁵ Ver (FCC, 2005)

⁶ Por el momento el regulador estadounidense ha defendido la neutralidad de red, pero hasta la fecha ha sido reacio a formalizarla normativamente. En febrero de 2004 su entonces presidente, Michael Powell, explicitó la política del organismo sobre la libertad en la Red. En un discurso en la Universidad de Colorado (EE UU) definió Internet como el derecho de los consumidores a una cuádruple libertad: de acceso a contenidos, de uso de aplicaciones, de conectar cualquier dispositivo y de recibir información sobre su plan de conexión a la Red

- **Sector privado.** Es aquí donde se manifiestan la mayor parte de las fricciones entre los agentes, ante las implicaciones económicas y de negocio que podría tener. De este modo existe una enorme rivalidad entre las empresas de servicios de Internet y los operadores de telecomunicaciones (proveedoras de acceso de banda ancha), por **tener el control final sobre el cliente.**
- **I+D.** El colectivo de I+D representa a los académicos e investigadores que participaron en la gestión de Internet y que con su trabajo a lo largo de los años han colaborado directamente en su evolución y desarrollo. La opinión más extendida es la de mantener la arquitectura tradicional como elemento clave que fomenta la innovación continua, sin perjuicio de explorar otras opciones ante el rápido desarrollo tecnológico y la evolución de los negocios en Internet.
- **Sociedad civil.** Numerosas asociaciones y ONG han manifestado su voluntad por una Internet neutral y que respete los derechos individuales, ya que esas cualidades han hecho de Internet el espacio público de creatividad e innovación que es en la actualidad. Son el colectivo más unido para hacer presión sobre los núcleos de poder y control aunque sus iniciativas son algo difusas.

Dadas las posiciones anteriores la principal cuestión es valorar la idoneidad o no de promover una legislación específica sobre la neutralidad de red o si bien debe ser una cuestión que quede en el plano de la gobernanza de Internet.

Parece lógico pensar por el análisis de los agentes anteriormente expuesto que dicha regulación no debería provenir de los organismos que vigilan la gestión de infraestructuras y recursos técnicos, ya que éstos precisamente tienen como misión el vigilar que se cumplan unas normas ya establecidas. Por lo tanto, la iniciativa de regular o no por ley la neutralidad provendría del resto de colectivos.

Esta cuestión entra en claro conflicto con las propias soberanías nacionales, ya que ante una cuestión de enorme complejidad como la que se plantea, que podría cambiar completamente el panorama económico y de negocio del sector TIC e Internet, podría darse el caso de que cada país adoptara una regulación propia en uno u otro sentido (acuerdo *de facto* vs norma *de iure*) que entrara en conflicto con una posición internacional concreta.

TEMAS DE ESTUDIO

¿Qué significa un cambio hacia la neutralidad de red? A priori un salto hacia la neutralidad de red supondría un cambio drástico en los modelos de negocio de telecomunicaciones y la comercialización de servicios y, lo que es más incierto, surgirían numerosas dudas sobre la sostenibilidad del cambio, particularmente ante la continua necesidad de inversiones para garantizar el futuro desarrollo de redes de nueva generación.

Al mismo tiempo debería conocerse si un cambio en el principio de neutralidad de red podría conllevar una modificación de las libertades individuales y colectivas que facilita Internet.

En cuanto a si debe regularse o no de la neutralidad de red, el reto radica en hacer

compatibles la esencia neutral y descentralizada de Internet, que ha hecho posible su gran desarrollo, y seguir avanzando en el despliegue de redes de banda ancha de alta capacidad que exigen inversiones sólo abordables en un escenario de rentabilidad adecuada.

Por todo ello, en el área de la neutralidad de red y la gobernanza de Internet, se propone abordar las siguientes cuestiones:

- Definir los diferentes escenarios que podrían configurarse debido a un cambio en el principio de neutralidad de red, desde un punto de vista económico, político y social.
- Valorar el papel de los colectivos involucrados en la adopción de los diferentes escenarios planteados.
- Proponer un escenario de futuro que garantice la sostenibilidad del negocio de las telecomunicaciones e Internet.
- Valorar las implicaciones que la neutralidad de red tiene en la regulación de las comunicaciones electrónica e Internet y la capacidad de los diferentes colectivos para influir en la adopción de un modelo concreto a nivel internacional.

SEGURIDAD, PRIVACIDAD Y CONFIANZA EN INTERNET

Internet ofrece grandes oportunidades para el avance de objetivos sociales, económicos y políticos, convirtiéndose en un espacio alternativo al mundo físico donde vender y ofrecer contenidos, servicios y bienes.

Internet constituye un entorno complejo, heterogéneo y cambiante en el que no tienen cabida los modelos tradicionales de autoridad. El poder se distribuye entre distintos sectores sin que ninguna entidad tenga control sobre cómo se produce este reparto. Cada red dentro del conjunto de redes interconectadas se encarga de su pequeña parcela, cada una de las cuales puede considerarse en realidad propiedad de varios agentes, y todos colaboran para lograr el acuerdo de un conjunto de reglas y estándares comunes.

En este contexto resulta difícil identificar quiénes deberían liderar la implantación de medidas que garanticen la seguridad en Internet ya que no existe una entidad con legitimidad para dirigir el desarrollo la Red. Todos estos factores hacen que sea muy difícil establecer responsabilidades y directrices. Los retos aparecen por tanto desde diferentes puntos de vista: legal, social, tecnológico, económico, político y cultural⁷.

Implementar la seguridad en Internet es una tarea complicada que exige que se pongan en marcha simultáneamente estrategias a distinto nivel y que implican a diferentes agentes. Esta coordinación necesaria para perseguir el objetivo de una red segura exige que se establezca un dialogo de cooperación entre los distintos sectores que juegan un papel importante.

⁷ Ver (Miller, G. et.al., 1999)

COLECTIVOS Y POSICIONES

A continuación se presentan las principales posiciones de los colectivos de agentes implicados en la gobernanza de Internet sobre la seguridad de la Red:

- **Sector Público.** Desde el sector público existe un claro interés por garantizar la seguridad de la Red. Los usuarios de Internet se enfrentan, por una parte, a fallos de seguridad relacionados con las tecnologías de la información, como los virus informáticos, y otros de origen social, como el fraude o el robo a través de Internet. Sin embargo, muchos de estos usuarios no son conscientes de los riesgos a los que se exponen.

Así cuestiones como el desarrollo de la eAdministración, que requiere de usuarios cómodos y confiados en el uso de aplicaciones en red. Por otra parte, en el contexto de la Nueva Economía resulta fundamental que se desarrolle el comercio electrónico y las empresas crezcan a través de Internet. En todo ello la confianza resulta ser un factor fundamental para fomentar el uso de las TIC e Internet. Con el desarrollo de los servicios electrónicos y las operaciones empresariales en red, la seguridad de la información y la confianza se convierten en requisitos para un negocio de éxito. El reto para las autoridades públicas es la creación de un entorno tal que fomente la seguridad necesaria sin imponer unas condiciones excesivas o costes excesivos.

El sector público es responsable de llevar a cabo iniciativas de sensibilización, de educación al público, de fomento de buenas prácticas en Internet, de incentivos a empresas del sector privado, de legislar adecuadamente y de garantizar que la ley se cumpla⁸.

- **Sector Privado.** En el sector privado los intereses por la seguridad de la red están directamente ligados a su propio modelo de negocio. Los proveedores de servicios de Internet y los servidores DNS son responsables del funcionamiento de la red y el crecimiento de Internet les beneficia directamente. Por lo tanto, tienen un interés directo en que la red mejore y llegue a cuantos más usuarios sea posible.

A los proveedores de servicios les preocupan todos los fallos de seguridad que pongan en peligro la viabilidad de Internet y aquellos que repercutan en la calidad del servicio que pueden ofrecer a sus clientes. Por ejemplo, el *spam* es una de las grandes preocupaciones del sector privado. Por su parte a los servidores DNS les preocupan los ataques de negación de servicio que pueden provocar tal exceso de tráfico que les obligue a interrumpir el servicio.

Por un lado, un proveedor de servicios estará interesado en ofrecer cierto nivel de seguridad a sus consumidores y tenderá a ignorar lo que ocurre fuera de su red. Sin embargo, ciertos riesgos a los que se exponen en Internet dependen más bien de la colaboración y el acuerdo al que lleguen para actuar según un código de conducta común, de forma que la red en global esté más protegida.

⁸ Ver (Racicot, M. et.al., 1997)

En la actualidad una de las teorías con más fuerza es precisamente la autorregulación del sector privado. En su mano está colaborar con las fuerzas de seguridad del estado, fortalecer a los usuarios proveyendo acceso a herramientas prácticas, promover costumbres responsables de negocio y educar al público.

- **I+D.** Las instituciones académicas y organizaciones privadas dedicadas al desarrollo tecnológico y a la investigación son también promotores de la seguridad en Internet. Desde este sector se tiene interés por una red de calidad que dé lugar al desarrollo de nuevas tecnologías.

Los diferentes agentes de I+D centran sus esfuerzos en el estudio de los fallos de seguridad desde un punto de vista técnico, identificando cuáles son los puntos débiles de la infraestructura de Internet. A partir de ahí se proponen soluciones y se desarrollan técnicas de protección. Estas instituciones están en buena posición para orientar al sector privado sobre las estrategias que deben seguirse para incrementar la seguridad en las redes.

- **Sociedad Civil.** Las asociaciones de consumidores y usuarios colaboran a su vez para que la red sea segura. Están interesados sobre todo en evitar los peligros y riesgos que Internet presenta para el usuario: los contenidos ilícitos, el *spam*, los virus y la protección de la información suponen algunas de las preocupaciones principales.

Por otra parte, los usuarios exigen también una Internet de mayor calidad. Consideran necesario que los contenidos sean, no sólo lícitos, sino también adecuados. Sería conveniente que existieran herramientas que permitieran seleccionar y adecuar los contenidos al público correspondiente, atendiendo a sectores específicos, como los niños.

Algunas iniciativas orientadas a la mejora de la seguridad nacen de la mano de asociaciones de carácter privado que son creadas con independencia del gobierno y de organismos internacionales. Por ejemplo, las organizaciones que han liderado el control de la calidad de los sitios *web* a través de las “marcas de confianza” cumplen con estas características⁹. También las líneas de atención surgen como mecanismos independientes que actúan como intermediarios entre la Administración y los usuarios.

En el tema de la seguridad, todos los implicados tienen intereses que apuntan en la misma dirección. Sin embargo, las diferentes soluciones que se presentan al mismo problema que todos perciben tienen implicaciones distintas según qué grupos y tendrán una acogida muy diferente en los sectores que se vean afectados. El establecimiento de objetivos comunes debe ser el resultado de un balance de los intereses de todos los involucrados.

La implementación de redes seguras exige un diálogo fluido y acuerdos de colaboración entre los distintos grupos que conforman cada uno de los sectores y entre

⁹ Ver (Industry Canada, 2006).

los sectores. Esto es necesario, por una parte, para que la red de Internet se desarrolle de forma satisfactoria para todos los implicados. Por otra parte, aún más importante, ninguno de los sectores por sí mismo tiene capacidad suficiente para poner en marcha las medidas de seguridad o tiene el poder necesario para garantizar que otros sectores adoptarán unas medidas impuestas.

Aunque es responsabilidad de los gobierno que la ley vigente se respete (también *online*), la naturaleza inconstante de las muchas actividades conducidas en Internet, sumado a la posibilidad de los participantes para permanecer anónimos y el aspecto internacional de la mayor parte de las transacciones en Internet, hacen que sea muy difícil detectar actividades ilegales y aplicar las leyes existentes. Se hace necesaria la colaboración del sector privado (implementación de tecnologías de seguridad), de la sociedad civil (por ejemplo, las ONG que ponen en marcha iniciativas orientadas a garantizar la seguridad) y de los centros de investigación y desarrollo (evolución de las tecnologías que permitan cubrir los fallos de seguridad).

La coordinación de las estrategias y la colaboración efectiva entre distintos grupos que persiguen los mismos objetivos y visión puede resultar difícil. El hecho de que surjan distintas organizaciones que buscan realizar la misma tarea puede suponer un obstáculo, pues ese exceso puede aumentar la confusión de los usuarios. Por ejemplo, un “sello de calidad” o “marca de confianza” será tanto más efectivo cuanto más se dé a conocer a los usuarios de Internet y mayor número de sitios web escojan unirse a esta iniciativa; en este contexto, la presencia de diferentes “sellos de calidad” entorpece la creación de una marca reconocida en la que los usuarios confíen.

Las leyes de carácter nacional resultan de difícil aplicación en Internet, un medio internacional en el que los delitos pueden fácilmente trascender las fronteras e infringir las leyes de distintos países. Deberían investigarse y proponerse medidas para combatir de forma global delitos que nacen en el entorno de Internet o que cobran una importancia especial en este ámbito, de forma que se eliminen los vacíos legales en torno al cibercrimen.

Generar confianza en el usuario exige que las medidas que se adopten desde otros sectores sean transparentes y que los criterios adoptados sean conocidos. La sociedad civil debe formar parte en el proceso de implantación de seguridad y debe estar al tanto de qué medidas se ponen en marcha y por qué.

Las ONG que ponen en marcha iniciativas de seguridad como el etiquetado de páginas *web* o la creación de líneas directas deben estar al tanto de otras entidades que están realizando la misma labor y deben promoverse alianzas desde otros sectores, por ejemplo, desde el sector público. Además, para que la labor de estas ONG sea efectiva deben asistir a otros colectivos en la consecución de sus fines.

La autorregulación destaca por ser una de las medidas con más potencial. Sin embargo, resulta necesaria la colaboración de otros sectores (usuarios, centros de investigación y desarrollo...) para que se desarrolle una seguridad que satisfaga las necesidades de todos los implicados. En este modelo el grupo crea las reglas para sí y es también responsable de que estas reglas se cumplan y se apliquen. La implicación de

otros sectores sería de colaboración a distintos niveles.

Es importante que las estrategias se adopten dentro de un marco de colaboración y acuerdo entre las empresas del sector, dado que la efectividad de las tecnologías que se proponen depende de que éstas se pongan en marcha de forma conjunta y mejoren la red de forma global. Además, el hecho de que los proveedores de servicios y los operadores de los servidores pongan en marcha técnicas de seguridad destinadas a proteger tanto el tráfico entrante como el tráfico saliente exige que esto se decida de forma común y con la convicción de que estas medidas resultarán beneficiosas.

TEMAS DE ESTUDIO

A pesar de la investigación que se está llevando a cabo en el terreno de la seguridad y de las tecnologías que hoy existen para mejorar la Red, la realidad es que garantizar la seguridad en Internet a día de hoy no es posible. Uno de los motivos es que ninguna de las tecnologías es totalmente efectiva. Otro motivo es que todas las medidas que pueden aportar avances significativos exigen la colaboración de diferentes sectores para su puesta en marcha.

Esto plantea un reto: la colaboración de los distintos sectores en la implantación de medidas de seguridad, tanto a nivel nacional como internacional.

Los foros internacionales deben ser un lugar de diálogo y encuentro entre distintas perspectivas con la voluntad firme de explorar las posibilidades que ofrecen las nuevas perspectivas. Los problemas que plantea Internet tienen carácter global y, por lo tanto, también deberán tenerlo las soluciones. Se debe estar al tanto de las acciones que se emprenden en otros países y considerar su efectividad y de qué forma serían adecuadas.

Algunas de las actividades que tienen especial interés dentro del marco de la seguridad en el ámbito de la gobernanza de Internet son:

- Elaborar una propuesta consensuada sobre los atributos y elementos que debe tener Internet para garantizar la seguridad, privacidad y confianza de sus usuarios.
- Analizar la conveniencia de desarrollar códigos de autorregulación a nivel nacional en el sector privado, coordinando estrategias que protejan a la red tanto a nivel nacional como internacional.
- Analizar la conveniencia de desarrollar códigos de autoconducta que respeten todos los usuarios de Internet, particularmente en la lucha contra la distribución de contenidos ilegales.
- Elaborar un plan de acción de seguridad de Internet, basado en tres ejes principales de actuación:
 - Sensibilización social. En esta tarea tiene una responsabilidad especial el gobierno, pero para informar apropiadamente a los ciudadanos se hace necesaria la participación del sector privado y asociaciones de usuarios

que además informen sobre los riesgos y las técnicas que están a su alcance para afrontarlos¹⁰.

- Cooperación multilateral entre colectivos. El negocio electrónico depende en gran medida de la seguridad de las redes, de la confianza de los usuarios y de la eficacia de ciertas tecnologías de autenticación y de firma digital. Para este sector es esencial partir de un punto de vista en común y desarrollar una estrategia que aumente la seguridad en el comercio a través de Internet.
- Colaboración con las fuerzas de seguridad del Estado en la lucha contra el cibercrimen. Desde el sector privado se puede ayudar a la detección de actividades ilegales y la identificación de los autores. El problema es que la razón de existir de esta colaboración no es tan evidente: los usuarios exigen que se respete su privacidad¹¹.

BRECHA DIGITAL

El desarrollo de la Sociedad de la Información supone una oportunidad para integrar los estamentos sociales más desfavorecidos en un nuevo modelo de sociedad, pero al mismo tiempo podría producir el nada deseable incremento de las diferencias sociales, la conocida brecha digital. Por este motivo, los gobiernos nacionales y las instituciones supranacionales, plenamente concienciados para eliminar posibles diferencias sociales, apuestan por la extensión de la Sociedad de la Información a todos los niveles, evitando en lo posible la exclusión de los más débiles. El reto es por tanto aprovechar el cambio consiguiendo el beneficio de todos.

El problema de la división digital es complejo y no existe una solución sencilla para él. La brecha digital se refiere a la diferencia en el acceso y la equidad en la experiencia tecnológica basada en categorías tales como los ingresos, el género, la ubicación geográfica o la educación recibida.

El término brecha digital no sólo se refiere a la diferencia entre los individuos sino también entre grupos familiares, empresas y áreas geográficas que tienen o no la oportunidad de acceder a las TIC e Internet y utilizarlas con fines diversos.

Por otro lado, la brecha no se refiere únicamente al acceso, sino también al uso y aprovechamiento inteligente de las TIC, y en especial de Internet, vinculado a la producción, comunicación, comercialización y administración.

Internet se ha posicionado como un eje fundamental de la sociedad y la economía, un bien común al servicio de todos. La brecha digital implica que aquellos "no informatizados e informados" no tienen la opción de participar en empleos que requieren de estos conocimientos, en estrategias de gobierno electrónico y de educación *online*.

¹⁰ Ver (Centre for Socio-legal Studies 2003)

¹¹ Ver (Cameron-Waller, 2001).

COLECTIVOS Y POSICIONES

La gobernanza de Internet juega un papel muy importante para solventar la brecha digital que requiere de la participación de todos los colectivos implicados. A continuación se presentan las principales posiciones de los colectivos de agentes implicados en la gobernanza de Internet sobre la brecha digital:

- **Sector Público.** El sector público, representado por la Administración pública, es uno de los principales colectivos involucrados en la reducción de la brecha digital en una determinada región. Su acción se centra principalmente en impulsar iniciativas que extiendan el acceso a Internet a los ciudadanos, fomentar la participación de todos en la era digital, y alentar una economía basada en el conocimiento a través de la formación y educación de los ciudadanos, y favorecer el desarrollo del comercio electrónico y la eAdministración como factores que estimulen a su vez el uso y adopción de Internet por parte de todos.

El sector público es responsable de llevar a cabo iniciativas que persigan los anteriores objetivos. Entre esas iniciativas destacan campañas de sensibilización, de educación y formación, incentivar las inversiones, crear un marco legislativo adecuado y garantizar un desarrollo óptimo.

- **Sector Privado.** El sector privado es un colectivo clave para favorecer el desarrollo de la Sociedad de la Información y colaborar en la reducción de la brecha digital. El mercado de la banda ancha está en plena expansión y crecimiento, aunque éste se centra inicialmente en las áreas de mayor interés comercial, dejando en un segundo plano a las regiones menos favorecidas, en donde las altas inversiones necesarias y la baja demanda potencial no incentivan la creación de una oferta para estos usuarios.

Por tanto el sector privado reclama un apoyo institucional mayor para recibir las ayudas necesarias que garanticen la presencia de infraestructuras y servicios de Internet en las regiones de bajo interés para el mercado. En esas condiciones el sector privado debe asumir un fuerte protagonismo pero siempre con el respaldo y el estímulo del sector público

- **I+D.** Este colectivo está especialmente sensibilizado con la problemática de la brecha digital. Por su clara vocación a la investigación y desarrollo, promueven la mejora de la formación en TIC de los ciudadanos y la difusión del conocimiento, colaborando en muchas ocasiones con programas y proyectos de cooperación y ayuda.
- **Sociedad Civil.** Este colectivo promueve numerosas iniciativas en el ámbito local para proveer de acceso a la tecnología y para ayudar a ponerla en práctica en las poblaciones insuficientemente servidas. Así mismo defienden la necesidad de la participación de todas las minorías, garantizando el pluralismo y la participación de todas las comunidades.

TEMAS DE ESTUDIO

Abordar la brecha digital está más allá de los límites de una única iniciativa. Si bien es importante que las organizaciones lleven a cabo proyectos de TIC comunitarios para satisfacer las necesidades de sus habitantes tanto como sea posible, las cuestiones que están en juego en las brechas digitales nacionales e internacionales son enormes, y las organizaciones deben cooperar para resolver los problemas en colaboración. Los programas del sector privado, universidades, y los esfuerzos filantrópicos también son vitales en dichas colaboraciones.

Dada la necesidad de la colaboración participativa de todos los estamentos y colectivos involucrados, dentro del marco de gobernanza de Internet se plantean las siguientes cuestiones para su estudio:

- Analizar el papel de los diferentes colectivos en el desarrollo de la Sociedad de la Información y la lucha contra la brecha digital.
- Valorar el grado de coordinación de las diferentes iniciativas a nivel regional, nacional e internacional para el desarrollo de la Sociedad de la Información.
- Proponer diferentes escenarios de financiación y sostenibilidad de las iniciativas anteriores para reducir la brecha digital.
- Analizar los posibles mecanismos que faciliten la participación de las minorías y colectivos desfavorecidos en Internet, particularmente en materia de creación de contenidos e integración social.

CONCLUSIONES

El presente documento pretende ampliar el debate de la gobernanza de Internet para incluir cuestiones adicionales que tienen gran relevancia para su desarrollo. Partiendo de un primer análisis básico del caso español, los resultados obtenidos muestran como la sostenibilidad económica debe ser considerada para abordar temas de gran trascendencia para el futuro desarrollo de Internet, tales como la neutralidad de red, la seguridad y la brecha digital.

Las tres cuestiones anteriores son objeto de estudio y análisis en multitud de foros internacionales pero habitualmente no consideran prioritaria la necesidad de garantizar la viabilidad y sostenibilidad económica de las iniciativas impulsadas a partir del debate de la gobernanza de Internet. Por ello y con motivo de la IGF Conference de Atenas, en este documento se plantean propuestas concretas que deberían servir para focalizar el debate durante los próximos meses y avanzar en el proceso de diálogo multilateral que promueva un modelo de gobernanza de Internet viable y sostenible.

REFERENCIAS

Comín, S (2006): *La net neutrality... ¿permitirá que se regule Internet?* Boletín de la Sociedad de la Información. Telefónica.

Drake, W (2006): *Internet Governance in transition: trends, challenges, and the global debate.*

FCC (2005): *The FCC's net neutrality guidelines.*

Finkelstein, L (1995): *What is global governance?* Global governance, vol.1, pp. 367-372.

Froomking, M (1997): *The Internet as a source of regulatory arbitrage. In borders in cyberspace.*

Froomking, M (2000): *Wrong turn in cyberspace: using ICANN to route around the APA and the Constitution.*

Industry Canada (2006): *Promoting safe, wise and responsible Internet use.*

Lessig, L (1999): *Code and others laws of cyberspace.*

Miller, G; Sinclair, G; Sutherland, D; Zilber, J (1999): *Regulation of the Internet. A technological perspective.*

Racicot, M; Hayes, M; Szibbo, A; Trudel, P (1997): *The Cyberspace is not a "No Law Land"*. A study of the issues of liability for content circulating on the Internet.

Rosenau, J (1992): *Governance order and change in world politics.* Cambridge University Press.

Centre for Socio-legal Studies (2003): *Website quality labelling.* University of Oxford. Comparative Media Law and Policy. Support for cooperation and coordination projects in Europe.

Wu, T. (2003): *Network Neutrality, Broadband Discrimination.*