LACIGF10 – 2 al 4 de agosto de 2017

Sesión 4. Ciberseguridad: avances, retrocesos, desafíos y tendencias desde una perspectiva de derechos humanos

Fecha: Miércoles 2 de agosto. 17:00 a 18:30

Moderador: Diego Morales – IPANDETEC

Panelistas:

- Martín Borgioli – Hiperderecho
- Shernon Osepa - Internet Society (ISOC)
- Maureen Hernandez - Internet Society (ISOC) Venezuela
- Ernesto Ibarra – Presidencia MX
- Maria Cristina Capelo, Facebook

Relatora: Alejandra Erramuspe – AGESIC Uruguay

Moderador remoto: Youth LACIGF

1. Introducción el tema

El objetivo de esta mesa redonda es sostener un diálogo interactivo y dinámico que brinde una evaluación de las prioridades y implicaciones de ciberseguridad en nuestra región, en las distintas dimensiones: técnicas, derechos humanos, rol de gobiernos y de los otros actores.

Hay aún mucho que avanzar en cuanto a construir la confianza, gestionar las ciber amenazas, compartir las experiencias nacionales y ofrecer modelos para construcción de capacidades. La necesidad de alinear las políticas y estrategias de ciberseguridad con el marco internacional de derechos humanos sigue siendo uno de los nudos centrales y se precisa mayor discusión multisectorial al respecto.

El tema de ciberseguridad sigue en la agenda del LACIGF, así como en las discusiones locales y globales de gobernanza de internet. Los últimos años estuvimos enfocados en los temas de vigilancia y privacidad para hablar de ciberseguridad. Más recientemente, se ha visto un crecimiento en nuestra región de los casos de restricciones o bloqueos de Internet, las limitaciones al uso del anonimato y la encriptación y la expansión indiscriminada de la vigilancia, muchas veces bajo un argumento de seguridad nacional.

2. Estructura para la sesión

- Mesa redonda
- 3 preguntas-clave, cada una con una ronda de 2’ por ponente, intercalando con preguntas y comentarios de la audiencia

3. Preguntas-clave

- Cuál es el principal avance, retroceso, o desafío en ciberseguridad en la región?

- Cuál es el panorama sobre las restricciones y bloqueos de Internet?
- Cuál es el impacto en la confianza de los usuarios en Internet para el futuro de Internet?
- Qué ejemplos de buenas prácticas en ciberseguridad tenemos en la región?
- ¿En qué aspectos se debe trabajar en la región para asegurar que las políticas y prácticas de ciberseguridad tomen como referente las recomendaciones de relatores de Naciones Unidas y OEA así como los marcos existentes a nivel internacional?
- ¿Cuál sería la manera más efectiva de contrarrestar la tendencia a aplicar restricciones o bloqueos de internet por parte de los gobiernos?
- ¿De qué maneras se puede avanzar en la construcción de la confianza en internet? ¿Qué condiciones se precisan en LAC para afianzar la confianza en internet?

4. Desarrollo del panel

El moderador comienza planteando cuál es el principal avance y el mayor retroceso de la ciberseguridad en la región y hasta donde es posible llegar.

Se señala que el principal avance está en que cada vez más se incluye las distintas voces, a partir de los modelos participativos se han abordado mejor estos temas, no solo a nivel tecnológico sino también cultural y jurídico.

Se indica que el principal retroceso que se ve en la región es la aparición de la vigilancia masiva dirigida a la ciudadanía. Es hipócrita demandar el enfoque de múltiples partes interesadas que puedan solucionar este problema. Hay que hacer un mea culpa y preguntarse sobre lo que estamos haciendo nosotros por mejorar nuestra ciberseguridad.

Se demanda que es preciso prestar atención a los derechos humanos: privacidad, libertad de expresión, derecho de buscar y recibir información y en esto hay un punto importante y es que se están viendo bloqueos, que es preciso evitar.

Un aspecto a tener en cuenta es el bloqueo de contenidos. ISOC trabaja en esto. Hay algunas cosas que suceden en la red y los gobiernos muchas veces quieren borrar estos fenómenos de la red, a saber: juegos de apuesta, desafíos de propiedad intelectual; protección de niños y niñas y también seguridad nacional. La ISOC puede ayudar a encontrar soluciones.

5 maneras de bloqueo que ISOC está viendo:

a. A nivel de Direcciones de IP o protocolos: se pueden colocar en una lista y pueden ser bloqueadas.

b. Deep Inspection: inspección profunda de los paquetes con técnicas específicas para atacar.

c. URL: conocer la ubicación de la información.

d. Platform biz: buscadores de información. Google por ejemplo. Hay otros.

e. Bloqueo a base del sistema de nombre de dominio

Se plantea que hay que tomar como referencia las sugerencias de las relatorías independientes, deben escucharse. Existen diferencias entre lo que opinan los gobiernos y lo que dicen las Organizaciones de DDHH.

Muchas veces los gobiernos colectan información de sus ciudadanos sin pedir autorización y sin que éstos lo sepan. Tiene que haber un propósito adaptado a los derechos humanos en estas acciones.

Desde la sociedad civil se plantea que es difícil hablar de confianza cuando hay un contexto de vulneración de derechos. La participación de la sociedad civil tiene que darse en un marco de garantía. Hoy no existe esa confianza.

Una buena práctica que pueda exportarse a la región es tomar la ciberseguridad con una visión estratégica, como una palanca para el desarrollo de la innovación. Promover la adopción de estos ejercicios de colaboración no solo en los planes sino en la implementación de las estrategias de ciberseguridad. Los desafíos de la ciberesguridad, son globales, por ello tenemos que trabajar todos juntos.

Se debe apostar por construir la confianza. Para la construcción de la confianza, hay que romper el paradigma de que la ciberseguridad es algo oscuro, hay que desmitificarlo, para que los usuarios estén abiertos a ser conscientes de este tema. Esa concientización puede darse a partir del conocimiento de las herramientas.

La ciberseguridad debe pasa por un compromiso de los gobiernos de defender a la población no solo de lo externo sino también en la adopción de la tecnología.

No somos conscientes de la falta de seguridad de muchas de las aplicaciones que usamos a diario.

De qué manera construir la confianza? Es muy difícil construir la confianza. Un sistema de datos abiertos sería bueno para la confianza. En los países que se recaban datos, debería haber leyes que protejan los datos. Si hubiese información más abierta sobre estos temas, los usuarios tendrían mayor confianza. También con más interacción para fortalecer la legislación y el marco institucional. Antes de implementar las políticas, antes de aprobar la legislación habría que discutir con la sociedad civil.

Moderador: Qué condiciones notan que se están dando en la región que pueden dañar la confianza?

Se habló sobre los 3 niveles de internet: infraestructura, DNS y las aplicaciones. Sostuvo que hay que buscar una solución holística y lograr acciones concretas.

Se planteó que muchas veces los usuarios a veces no saben cuándo están poniendo en riesgo su seguridad por eso es necesario trabajar con el sistema educativo, para tener conductas de prevención. Y en esto es categórica la acción de la sociedad civil.

Algunos políticos o creadores de políticas no tienen formación en temas de tecnología, por ello es importante que estos actores tengan la capacidad para darle a la ciudadanía la confianza necesaria. En las últimas décadas la aparición de políticas digitales, marca un parte aguas respecto del uso responsable de internet y de las tic. Por lo tanto es preciso contar con una alianza de diferentes actores para incidir en esto. Iniciativas de gobernanza de internet que se desarrollan a nivel de cada país son importantes.

Trabajando cada vez más en estos temas de forma abierta y transparente ayudaría porque la cooperación y la corresponsabilidad aportan mayor valor.

Participación del público

- Cuál es la forma y el proceso de adopción de políticas públicas por parte de los gobiernos, a veces no hay compromiso de los gobiernos. Preocupación genuina entre lo que es seguro, lo que es privado y lo que es abierto. Necesitamos un cifrado que permita proteger los datos. Como pueden integrar los gobiernos estos conceptos?
- Participación ciudadana y construcción de evidencia que permita a los entes públicos la construcción de una política pública más acorde. Empoderamiento de la sociedad civil y la academia así como la participación, es la parte de un ciclo que va nutriendo constantemente la política pública. Fortalecimiento de la labor jurisdiccional.
- LACRALO: En Latinoamérica tenemos una red de 52 organizaciones, distribuidas en 21 países que hacemos adiestramiento para los usuarios finales de internet. Dado que los gobiernos no bajan línea tenemos que hacerla nosotros, de abajo para arriba.
- La tecnología va a ayudar a mejorar la seguridad. Al mismo tiempo hay que apostar al aspecto cultural.
- La ciberseguridad es presentada como algo oscuro, pero esto no es así. Ciberseguridad es algo que tiene que tener un enfoque, una perspectiva más cercana
- En Perú existe una política de datos personales. Hay una división de la policía que se encarga de estos temas, también hay un CERT. El acercamiento es necesario, la ciberseguridad debe ser algo pensado para todos.
- Se plantea que hay que tomar el tema de seguridad de las mujeres y de los activistas en la red que muchas veces no es tenido en cuenta.
- Los usuarios no saben cómo se encripta.