Sesión 1: Vigilancia y privacidad: Las preocupaciones sobre la ciberseguridad y la confianza en el entorno digital

Moderación: Maricarmen Sequera - TEDIC, Paraguay /
Cédric Laurant - Son tus Datos, México

Panelistas:

Sociedad civil: Katitza Rodríguez -Electronic Frontier Foundation, Perú
Gisela Pérez de Acha - Derechos Digitales, México
Sector privado: Ana Lucía Lenis - Google
Fernando López - ASIET
Comunidad técnica: Julián Dunayevich -NIC Argentina, Argentina

Moderador remoto: Daniela Viteri - Universidad San Francisco de Quito, Ecuador

Relator: Leandro Ucciferri - Asociación por los Derechos Civiles, Argentina

---

Parte I

Comienza Maricarmen Sequera moderando el panel. Se dividen los paneles en grupos. Primero explicando el contexto, dónde estamos, qué es ciberseguridad, la creciente digitalización de la diversidad de dimensiones de la vida social, económica, política, cultura, y el crecimiento de los intereses de los distintos actores (gubernamentales, sociedad civil, academia, comunidad técnica, sector privado). Ciberseguridad desde el reconocimiento del acceso a internet, que ha vuelta más complejas las amenazas a los datos que circulan por las infraestructuras de Internet, y las respuestas legales en torno a las mismas.

Cómo preservar el carácter libre, seguro, abierto de Internet. Por qué prevalece que hay que sacrificar los DDHH si se quiere lograr ciberseguridad. Cuáles son las políticas públicas que se necesitan desarrollar para garantizar la ciberseguridad sin perjuicio de afectar los DDHH.

Ana Lucía Lenis: Comienza por la primer pregunta, cómo preservar el carácter abierto, libre, la seguridad en Internet. Resalta que para trabajar en este tema se debe ver la ciberseguridad como un tema multistakeholder. Desde Google ven que el debate en la región en muchos casos se confunde la ciberseguridad con el ciberdelito, la parte estrictamente penal, de tipificación de conducta a través del trabajo legislativo. Se ve la ciberseguridad como una conversación entre industria y gobierno, y no como un espacio donde deben tener voz todos los actores. Es un tema donde hay que seguir trabajando, no es un tema estrictamente entre dos actores, sino abierto sobre todo los derechos fundamentales de los ciudadanos. Es muy relevante para la academia y la sociedad civil.

En los debates que se dan en el legislativo se ve un gran desconocimiento cuando se legisla sobre estos temas. Ahí debe ponerse en relevancia a la comunidad académica y técnica, para asesorar a legisladores.

La seguridad de los usuarios es una responsabilidad compartida, que debe comenzar por la educación. Muchos de los ataques que sufren los ciudadanos es por desconocimiento de las medidas que pueden tomar para protegerse.

En relación a los delitos informáticos, se ve claro el factor de la territorialidad, donde estos no reconocen fronteras. Deben tipificarse de manera correcta para evitar que ciertas actividades sean declaradas ilícitas por desconocimiento del legislador.

Katitza Rodríguez: En el tema de ciberseguridad el gran problema es que no hay claridad en las prioridades con lo que significa la seguridad digital, el concepto es muy nebuloso y significa muchas cosas para distintas personas. Mezcla como un concepto monolítico, con cuestiones distintas que requieren soluciones distintas. Esta necesita medidas necesarias para que la economía se fortalezca. Se necesitan políticas claras con análisis de riesgos claros, con necesidades específicas para medir la proporcionalidad de las medidas. Una buena forma de proteger la seguridad digital, es necesario que la infraestructura sea segura, y usen cifrado fuerte punto a punto. Resulta irónico que a pesar de que se busque proteger la seguridad digital, se vean políticas públicas que buscan socavar la misma seguridad creando por ejemplo backdoors. Entonces en vez de promocionar el cifrado se buscan promocionar políticas públicas que lo minimiza.

Como proteger el carácter libre y abierto de Internet? Todas las normas de carácter penal y de políticas públicas, busquen garantizar que las medidas que se adopten sean necesarias proporcionales e idóneas, que sean razonables. Para ello la sociedad civil desarrollamos los 13 principios internacionales para la promoción de los derechos humanos en la interceptación de las comunicaciones, para cumplir con los estándares internacionales de DDHH y debido proceso. EFF junto a Derechos Digitales lanzaron un informe de análisis de estos principios en el marco de los estándares internacionales de DDHH.

Gisela Pérez de Acha: Está de acuerdo que el concepto de ciberseguridad es nebuloso. Cada vez que se usa la palabra “ciber” tiene cada vez menos significado, otorgándole sensacionalismo al tema de la ciberseguridad, que en la región se ha visto que se usa para socavar DDHH. Propone acotar a cómo afecta la ciberseguridad a temáticas de género. La definición que proponen es la preservación a través de políticas y educación de la infraestructura crítica subyacente tanto online como offline, el objetivo es proteger la integridad de las personas.

Dividen en dos rasgos: Cibercrimenes y crímenes en cuanto a contenido (toda la discusión de derechos de autor deben dejarse fuera del debate de ciberseguridad); Y seguridad nacional, lo cual también es un concepto abusado, se debe poner énfasis en cómo se usa el mismo.

Menciona el caso de Spúlveda, el hacker que intervino en las elecciones de Colombia.

Cómo preservar la infraestructura crítica: se debe considerar qué organismo va a ser el encargado de investigar estas acciones.

Menciona el caso de una base de datos filtrada con datos de la población mexicana subida a un servidor de Amazon Cloud, y el rol de la empresa ante la solicitud de baja de ese contenido.

Qué pasa cuando los dañados son los grupos vulnerables, LGBT, mujeres por temas de género?

En Internet hay un bien fuera del dinero que son los cuerpos, sobre todo los cuerpos desnudos y más aún los disidentes. Para ciertos atacantes son un bien muy valioso. De ahí surge el fenómeno de la "sextorsión", hackers criminales que acceden a las webcams grabando y buscan pedir dinero por ello. Una gran parte de las personas afectadas es menor de edad.

Cómo cambiar el foco de la ciberseguridad entendida en cibercrímenes, para también incluir a los cuerpos e identidades.

Fernando López: La concepción de políticas públicas no encaja con los problemas del sector. Hablamos de regulación que teóricamente tiene un enfoque diferente. Donde no solo participa el Estado o gobierno, sino que participa un ente con distinta calidad de autonomía que debe relacionarse con personas del sector privado, la sociedad civil. Por eso estos foros de gobernanza son tan importantes.

Desde el análisis de las políticas públicas, lo primero que se plantea es que la regulación llega tarde a la concepción de problemas públicos. Nos damos cuenta que debemos resolver algo cuando estos se vuelven evidentes para todos y supera la manera en que entendemos los problemas.

La realidad que hoy vivimos es muy distinta a la pasada. Los modelos regulatorios se están transformando, pero no han logrado atender a las necesidades de los usuarios.

Aun no queda claro cuál es la función que debe desempeñar cada uno de los actores. El gobierno trata de asumirlos, pero en ocasiones se vuelve parte del problema. En tal sentido, la preocupación principal es cuál debe ser la alternativa más importante para que el ecosistema se siga desarrollando.

Cree que hay coincidencia en que se debe partir desde el usuario. Como garantizar que se le respeten sus derechos y se sienta seguro al utilizar las tecnologías. En la medida en que este gana confianza, esto se traslada en innovación, ampliación de la capacidad de acceso a más personas. Pero para ello se requiere seguir avanzando firmemente en base de un conocimiento real de lo que está sucediendo y la interacción de los usuarios con nuevas tecnologías.

Es fundamental que los gobiernos sean capaces de plantearse cuáles son las medidas que fueron adoptadas, y como dar la certidumbre necesaria para que las personas puedan seguir alimentando el desarrollo de las telecomunicaciones y seguirse informando.

Estamos hoy ante una sociedad más consciente que poco a poco exige más garantías en la manera en que las propias autoridades pueden permitirle desarrollar sus actividades en la red de una manera segura. Ahí es fundamental la educación. Fortalecer a los usuarios para que conozcan sus propios derechos, y en función de eso tengan las herramientas para hacerlos valer.

Tradicionalmente las empresas de telecomunicaciones están obligadas a proteger la información y los datos de las personas, y existe un esquema para cuando estas se violan. Pero a medida que salen nuevos servicios no hay criterios que permitan proteger la seguridad del usuario.

Se debe exigir en el ecosistema digita lo mismo a todos los actores. Ya que sino el riesgo permanece. Es fundamental repensar en la industria el valor de los datos personales, y los servicios que se ofrecen de manera gratuita, tienen considerado un costo específico en el usuario al momento en que ofrecen sus datos. Puede ser que el usuario esté dispuesto a compartirlo, pero en la mayoría de las veces el usuario lo ignora.

Es importante comenzar a plantearnos la manera en que nosotros como grupos especializados podamos transferir esa información a los usuarios para que puedan decidir. Que sean el centro de las prácticas y políticas regulatorias. Y tengan la posibilidad de estar conscientes sobre lo que pueden hacer. Ya que no resulta claro a quién pueden acudir o suspender la utilización de sus datos. A veces no resulta claro qué normas aplican a servicios que tienen carácter global. Es necesario que se haga un debate para el ciudadano de a pie.

Debe asumirse de manera abierta y contemplarse las alternativas para tener un internet abierto bajo el que se respeten los DDHH y que las políticas públicas lo sustenten.

Julián Dunayevich: Comienza con los desafíos del trabajo de la ciberseguridad desde el punto de vista como ccTLD. Deben tener herramientas, directrices y métodos para defenderse de ataques y responder ante denuncias. Como toda infraestructura, son críticas como otros sectores (energía, agua), lo llevan adelante desde distintas áreas, todos en su lugar deben llevar adelante la gestión de los trámites de dominio y cuidar la infraestructura que si se cae tiene un impacto importante en Internet y los países.

Resaltan los diferentes proyectos y abordajes que tienen: la robustez de la infraestructura que deben manejar. LACTLD lleva a cabo un proyecto para compartir infraestructura entre los distintos países de la región para que tengan mayor robustez y trabajar de manera colaborativa entre todos.

Otro factor de ataque es en los clientes, entre la consulta y la respuesta del servidor. Trabajan en que el navegador tenga mayor certeza al momento de contestar sobre una URL que no sea malintencionada.

Debido a la robustez de las infraestructuras están preparados para realizar “disaster recovery”.

La ciberseguridad hace a la necesidad de trabajar con las múltiples partes interesadas. Cada uno de ellos puede participar de la solución de esto. Por ello es fundamental trabajar con los distintos sectores, en forma coordinada, tanto nacional como regionalmente.

Ámbitos de competencia en cuanto a la ciberseguridad, ellos deben trabajar con cada una de las áreas que deben actuar ante denuncias y definir los pasos a seguir. Ante lo cual hay que plantear protocolos.

Los diferentes ccTLD tienen grupos que deben actuar frente a incidentes de ciberseguridad, en los que reciben muchas denuncias. Tienen la oportunidad de articular con otros grupos regionales que les permite generar una base de conocimiento sobre cómo encarar el incidente. Destaca que tienen una ventaja, ya que al recibir las denuncias ya tienen ciertas denuncias para actuar frente al problema, por ejemplo la información de contacto de cada uno de los dominios, lo que les permite actuar más rápido con el titular y dar una solución más expeditiva, siempre en el marco de lo que defina la justicia no en forma unilateral.

Tienen protocolos y mecanismos de acción en temas de: ámbitos de incumbencia y competencia (por ejemplo si la IP pertenece a otro país, o el dominio donde reciben la denuncia no tiene nada que ver con su ccTLD, a lo que trasladan el incidente a quien corresponda), categorización de los incidentes, canales de reporte y notificación, alcances y acciones.

Tienen una categorización de los distintos incidentes, y a partir del conocimiento de estos se puede trasladar la información a la justicia para que siga con el proceso.

Como ccTLD, ven importante proteger sus infraestructuras, la colaboración e intercambio de experiencias, tener políticas compartidas, tener un modelo de ciberseguridad regional y ponerse de acuerdo para encarar estas situaciones, y tener sistemas de información confiables que les permitan trabajar más rápido.

Cédric Laurant: interviene preguntando a los panelistas para luego dar la palabra al público.

Comienza con Ana Lucía. El sector privado debe fomentar la confianza de los usuarios. En México, Uruguay, Costa Rica y Colombia, la entidad de protección debe fomentar la confianza demostrando que las empresas tienen las medidas para que al momento de vulneración de los datos saben cómo responder. Cuál sería la medida a tomar?

Ana Lucía: Se tiene que acotar a las bases de datos de esos países. Cualquier notificación debe darse bajo cumplimiento estricto de la ley. Muchas bases de datos no se encuentran en esos países. En Google recomiendan en cuanto a publicación sobre incidentes, en muchos casos la colaboración se entre empresas del sector privado, compartiendo información hacia el Estado, pero falta trabajar desde el otro lado, qué riesgos ven los Estados que puedan compartir al sector privado para estar mejor preparados. Desde la aplicación de regulación de cada país, debe verse caso a caso.

Pregunta a Katitza: sobre cifrado punto a punto, cuál sería la medida más efectiva para promover este uso?

No se está pidiendo legislación, sino se busca educación pública, que se entienda los riesgos de usar la tecnología. Que la gente use la tecnología, pero explicando los riesgos. Una forma de defender de ellos es el cifrado. El cifrado te permite comunicaciones seguras. Este tipo de cifrado debe masificarse con educación pública y políticas públicas. En campañas del día de la ciberseguridad no se vio comentarios por el uso del cifrado.

Cédric: En una reciente campaña promovida se recomienda no hacer sexting, pero se olvidó que no es una práctica que va a desaparecer y que no es mala. No se habló del uso del cifrado de los contenidos del celular ni de los mensajes.

Gisela: Distingue el sexting como una práctica consensuada, de la sextorsión o pornovenganza y el abuso de imágenes. El cifrado impediría o haría más difícil que estos contenidos sean accedidos por terceros. Sobre todo que no se prohíba el anonimato o el cifrado de las comunicaciones con fines de proteger contra el cibercrimen.

Pregunta del público:

Renata Aquino (Brasil): Pide relacionar en casos de América Latina y buscar la solución.

Katitza: En EFF publicamos una guía de protección contra la vigilancia contra quien sea tu agresor. Profesores, activistas o simplemente un ciudadano contra delincuentes. Esta te enseña a realizar un análisis de riesgo, cómo proteger la información en un caso concreto. No se puede proteger todo de todos, se debe realizar un análisis del caso concreto. El sitio web es https://ssd.eff.org

Parte II

Eduardo Rojas (Fundación Redes): Cuáles son las perspectivas y recomendaciones en torno a posibles métodos para enfrentar las olas de reformas legislativas en los países, ciberseguridad, regulación de redes sociales, grooming, etc Hay una confunsión de proteger el bien patrimonial de la defensa de la persona.

Ana Lucía Lenis: Vemos un auge de multiples procesos legislativos en toda la región. La visión del sector privado es aprovechar estos foros de gobernanza de Internet para encausar el debate de proyectos legislativos, estos temas deben tratarse por múltiples partes , un buen ejemplo son los foros locales de gobernanza, caso de México, el foro Colombiano. Trasladar esos debates locales, invitando a universidades y otros actores, para poder influir en el país.

Katitza: La experiencia comparada es buena y hay buenas prácticas. En ciberseguridad la OECD publicó un reporte, que es un ejemplo de un paper escrito multistakeholder, con una visión que trata de promover este análisis de riesgo de lo que se quiere proteger, de quién y

cómo, para realizar una política pública que solucione ese riesgo específico y que sea proporcional y razonable.

Gisela: Mantener el derecho penal al mínimo. Sobre todo en las cárceles latinoamericanas, meter más leña al fuego resultaría excesivo.

Fernando: Menciona el caso de la Ley Fayad. Gracias a la sociedad civil se logró un proceso de consulta abierta.

Pregunta Manuel Alcántara: Resalta la confusión de ciberseguridad y ciberdelitos. Pregunta a Ana Lucía compartir una definición más diferenciadora de los términos, o ejemplos que ayuden a delimitar la delgada línea que las separa. Pregunta a Julian si puede compartir recomendaciones sobre la correcta conformación de un centro de respuesta ante incidentes, y qué método o protocolo siguen en NIC Argentina para remitir la prueba a la justicia.

Ana Lucía: Cuando participan en los debates desde el sector privado, ven que muchas personas se enfocan en la ciberseguridad desde el punto de vista de los delitos informáticos, lo ven desde la penalización y criminalización de comportamientos, y no todo el debate que está en torno a todos los actores que deben trabajar la temática. Se olviden de las otras visiones, comenzando sobre la propia educación de los ciudadanos. Sobre todo teniendo en cuenta los derechos fundamentales, debido proceso.

Julián: En relación a la construcción del CSIRT, es fundamental comprender el alcance de cada uno de los actores y definir convenios con ellos. Debe involucrarse a la mayor cantidad de personas en el debate de la temática. En muchos casos, un mal procedimiento lo que hace es corromper la evidencia, por eso deben definirse los procedimientos en cada caso. Como ccTLD tienen un área de incumbencia muy específica, por lo que es fundamental articular con todas las partes, incluso armar CSIRT nacionales que puedan tener toda esa visión y actuar rápidamente.

Salvador Camacho (ISCO México): Pregunta para Julián, qué hace NIC Argentina para bajar la tasa de cyber squatting, y cuál es el nivel de conocimiento de los fiscales que persiguen estos delitos en Argentina?

Julián: Hay áreas específicas a nivel Ciudad, también a nivel Nación, y las Policías. Por lo que se puede trabajar con cada una de ellas. A veces trabajamos ese tipo de políticas, que no se generen nombres de dominios que se utilicen para atacar, porque cuando uno genera listas de nombres que no pueden ser justificados es una línea muy delicada.

Pregunta: es real la presunción de que la vulnerabilidad pesa sobre los usuarios?

Ana Lucía: El usuario es precisamente el reto que enfrentan las empresas, darles mayores controles para que ellos tomen las decisiones que quieren con sus datos. Es más un tema de educación que de bloquear el acceso a la innovación. Cuando se habla de protección de la privacidad de los datos de los usuarios, no es una discusión entre empresas de comunicaciones, OTT, etc, sino que en primer lugar, muchas regulaciones y empresas fueron

creadas antes de las leyes de habeas data y protección de datos. Es un tema que la industria debe tratar en conjunto. Destaca los cambios de seguridad que ha realizado Google sobre Android para brindarle mayor control al usuario sobre los permisos de las aplicaciones. La información que se recolecta es una información minimizada, con la cual se busca solucionar un problema del usuario.

Katitza: desde la sociedad civil no estamos diciendo que no utilicemos las tecnologías, le estamos diciendo a las empresas que quiero tener control sobre mis datos, que se puedan eliminar, cuál es su proceso de anonimización, cuánto tiempo son almacenados. Hemos visto que es muy fácil identificar a una persona en base a datos anonimizados.

Fernando: Le preocupa el lenguaje cuando se habla del tema. No pone en duda si son vulnerable o no, o si puede decidir o no. Sino que debe existir la posibilidad por parte de las personas de tener información y decidir de manera consciente y de manera práctica. Hay personas que pueden no ser conscientes de cómo son utilizados sus datos por las empresas que los recolectan. Remarca el conocimiento que deben tener los usuarios sobre las políticas de privacidad y el derecho a tener la información suficiente para tomar decisiones.

Ana Lucía: No vemos que debamos atacarnos dentro del mismo ecosistema, ya que dependemos uno del otro. Todo es mejorable. El tema de las políticas de privacidad y términos y condiciones es responsabilidad de todas las partes. Tenemos equipos trabajando para que las personas tengan información más clara.

Katitza: El sector privado intenta proteger la privacidad, el gran problema es la recolección masiva de datos, y una vez que estos existen se pueden entregar al gobierno. Eso es un riesgo. Mayor recolección datos, mayor información retenida, mayor información que se pueden entregar al gobierno.

Pregunta: Cuáles serían las acciones que deben tomar las empresas de telecomunicaciones y el gobierno, en qué momento se vuelve una problemática para las mujeres?

Gisela: Como primer enfoque, no se debe culpabilizar a las víctimas, “Efecto mini-falda”. Haciendo en el sexting, no deben apoyarse iniciativas de tomar la sexualidad como algo malo y terrible que hay que abolir y prohibir fuera de internet. El riesgo del sexting es que terceros divulguen tu información sin tu consentimiento. Las distintas autoridades no saben cómo reaccionar ante esto. El enfoque es en vez de prohibir la sexualidad, educar sobre los riesgos. Deben incluirse los temas de género en todas estas agendas que se están dejando de lado.

Jessica (Intermundi): Cómo el dinero sigue decidiendo qué es importante en Internet. Remarca la hipocresía en el manejo de las palabras, que la empresas dueñas de la información tengan la misma responsabilidad que los gobiernos, los usuarios, etc. Qué tipo de políticas toman para que las empresas en su responsabilidad no hostiguen al ciudadano que puede o no leer o comprender las políticas de privacidad, etc, para que no sucedean. Si están conscientes del hostigamiento que hacen?

Katitza: Existen muchas herramientas. Justamente las leyes de protección de datos buscan equiparar el desnivel de las empresas con los individuos/usuarios. Esto no es una tendencia en la región. También hay herramientas propias que se pueden tomar, bloqueando información en Internet. Por ejemplo Privacy Badger, navegar anónimamente en Internet, navegar de manera segura, y guías para aprender herramientas para tomar control sobre sus datos. Dos estrategias, una legal y otra individual.

Pregunta: Que impacto se puede tener desde la sociedad civil fuera de la concientización y la incidencia?

Katitza: Se busca que la gente en general pueda salir a hacer campañas para proteger sus derechos, no solo organizaciones. No todo se trata de educación.

Oscar Robles (LACNIC): En el desafío de generar confianza es multistakeholder, cada grupo tiene su propia responsabilidad. La comunidad técnica genera protocolos de cifrado por ejemplo, y así con cada uno de los sectores. Como podemos nosotros como organismo multistakeholder, hacer algo para atender justamente al más vulnerable de esta relación que es el usuario final?

Julián: Es fundamental capacitar y formar a todas las áreas que desarrollan la legislación. Es común que los jueces no entiendan como deben tratarse estos temas, e incluso en las áreas de gobierno. Ven de lo que viene desde las áreas de la justicia el desconocimiento que existe.

Pregunta: Tomando el marco civil como referencia, como se puede atacar que no se trata solo de educación a usuarios sino también a jueces?

Fernando: Deben hacerse políticas más transversales, debido a las dificultades de la integración.

Katitza: varias organizaciones hacen informes en las que arrojan resultados específicos.

Monica Arroyo (Observatorio de la Juventud): Pregunta enfocada desde el derecho a la información. Se piensan en tratar de buscar eficacia en la información evitando páginas y páginas de términos y condiciones?

Katitza: Ninguna empresa va a decir que no quiere políticas de privacidad. Lo que tratan de hacer es explicar sencillamente el contrato. Hay problemas porque cuando quieres saber qué hace la empresa sobre tus datos no te lo dicen expresamente. En Perú se utiliza la ley de protección de datos para censurar ciudadanos.

Gisela: El consentimiento debe ser libre e informado, sino no es consentimiento. Los contratos de términos y condiciones no son ni libres ni informados.

Presentación de Gisela – Hacking Team en América Latina

El software que vende Hacking Team se llama Galileo. Es como tener un funcionario pública mirando todo el tiempo lo que hacemos en nuestros dispositivos y copiándolo.

En Ecuador hay pruebas que el software fue utilizado para espiar a Carlos Figueroa.

En Colombia la DEA estaba interceptando todo el tráfico de Internet.

En México las que compraron no tenían facultades para utilizar el software. Fue el país de América Latina que más gastó en la compra del software.

En Chile la policía de investigaciones decía en los correos que querían este software para ir más allá en sus investigaciones judiciales.

Salvo México y Colombia, en el resto de la región, va en contra de los estándares legales de cada país.

También encontramos PackRat y FinFisher.
Debemos preguntarnos cuál es el rol del malware en el papel de la ciberseguridad, y cuál es el papel del sector privado. Cómo el término “surveillance capitalism”, comienzan a predecir a dónde queremos ir, qué queremos buscar, cómo esto alimenta a las grandes empresas y al gobierno.

Y qué responsabilidad van a tener Hacking Team, PackRat y FinFisher, dado que nuestras leyes no los permiten.

El malware es una de las mayores herramientas para callar la disidencia.