LA SEGURIDAD DE LOS DATOS PERSONALES EN INTERNET Y LAS REDES SOCIALES
https://youtu.be/wD7AjqMQksQ?list=PLZaXWcGPIGDZKdmIwg2JDz58py_DDqjp5

PANEL 1 "LA SEGURIDAD DE LOS DATOS PERSONALES EN INTERNET Y LAS REDES SOCIALES"

Presentador: Para continuar, daremos inicio al Panel: "La Seguridad de los Datos Personales en Internet y en las Redes Sociales".

Este panel lo integran representantes de las organizaciones de la sociedad civil.

Tenemos en este panel a Katitza Rodríguez, de Electronic Frontier Foundation; Ferber Sánchez, de Latinoamericanos integrantes del Taller "Mapas de Rancho Electrónico"; Jesús Robles Maloof, de Contingente MX; Jorge Flores Fernández, de Pantallas Amigas; Paulina Gutiérrez, de Artículo 19 y; Carlos Martínez Velázquez, de Ciudadano y Consumidor.

Modera este panel el Comisionado Ciudadano del InfoDF, licenciado Alejandro Torres Rogelio, a quien le cedemos el uso de la palabra.

Lic. Alejandro Torres Rogelio: Muchas gracias, muy buenas tardes, gracias por continuar con nosotros en este día en que celebramos la protección de los datos personales, muchas gracias a quienes han aceptado participar en este panel con este tema que, tenemos además como antecedente lo que nos han manifestado los representantes tanto de Google, como de Microsoft.

Y para esta ocasión vamos a tener la participación de todos ustedes con este tema general, pero seguramente ustedes le darán el enfoque particular que desde sus organizaciones realizan cotidianamente para el tema de la seguridad de los datos personales en Internet y las redes sociales.

En primer lugar, le voy a ceder el uso de la palabra a Katitza Rodríguez, quien es Directora Internacional de los derechos de la Electronic Frontier Foundation, la EFF, ella se concentra en la política comparada de asuntos internacionales de privacidad, con especial énfasis en la aplicación de la ley, la vigilancia del gobierno y los flujos de datos fronterizos, transfronterizos; su trabajo en el programa internacional de la Fundación se centra también en la seguridad cibernética, en la intersección de los derechos humanos; ha sido asesora del foro de gobernanza de Internet de las Naciones Unidas y miembro del Consejo Asesor de Privacy International.

Antes de unirse a la Fundación, Catitza fue Directora del Programa de Privacidad Internacional de la Electronic Privacy Information Center en Washington, D.C. donde, entre otras cosas, trabajó en la privacidad y el informe de derechos humanos, que es una encuesta internacional de derecho y desarrollo de la privacidad.

Catitza es muy reconocida en las organizaciones de la sociedad civil a nivel internacional y en los lugares donde también se analiza la política internacional por su trabajo en la gobernanza de Internet de la ONU; ella es licenciada en derecho por la Universidad de Lima, Perú.

Le damos el uso de la palabra, muchísimas gracias por acompañarnos hoy, Katitza.

Katitza Rodríguez: Gracias, muy amables por la invitación, estoy muy contenta de estar aquí en México y muy agradecida con el InfoDF por su gentil invitación y a todos los comisionados y comisionadas por su invitación.

Para aquellos que no conozcan a mi organización, quería presentarme un poquito. Mi organización se llama o la organización donde trabajo se llama Electronic Frontier Foundation IEFEF, es un estudio de abogados por el interés público, hacemos litigio estratégico demandándose a grandes corporaciones o a gobiernos.

Uno de los casos más famosos que tenemos en estos momentos, por ejemplo, es una demanda contra la Agencia de Seguridad Nacional de los Estados Unidos por la vigilancia, el espionaje que realiza a personas inocentes no sospechosas de delito alguno.

Pero también trabajamos temas de libertad de expresión, peleando legalmente y en temas de censura en la red, sean temas de derechos de autor… digital cuando estas normas se usan para censurar las actividades de los usuarios de Internet, o sea promoviendo normas que promuevan el tipo de usos justos de normas que esas excepciones y límites a los derechos de autor que permite que los usuarios puedan innovar usando la tecnología.

Pero no solo somos un estudio de abogados que además nos fundamos hace varios años, en 1990, sino que además somos un grupo de activistas, de comunicadores que explican a nuestra mamá y a nuestro papá cómo funciona o de qué se tratan estos temas.

La idea es que podamos masificar y explicar de manera sencilla la intersección de los derechos humanos y la tecnología, para que mamá y papá puedan comprenderlo.

Y también tenemos equipos de tecnólogos, de expertos en seguridad que hacen herramientas que permiten navegar a ustedes de manera segura, hacer un *playing* que permita la navegación de Internet de manera segura y otras herramientas que se han masificado, se han vuelto muy populares a nivel mundial.

En mi persona, yo soy responsable del área políticas públicas para América Latina y Directora del área de Vigilancia y Derechos Humanos para la IEFEF.

Hoy día estoy terminando un trabajo que busca comparar las normas de vigilancia estatal, de espionaje en América Latina o en las Américas, en 13 países de la región: Sudamérica, Centro América, cuatro países de Centro América, México y también tenemos Estados Unidos.

Y de eso, uno de los temas que resalto o que aún no publicamos, pero les doy un avance, uno de los resultados más grandes es el avance que se está dando al tema del uso del Software malicioso, ese Software que es usado para capturar tu computadora, lo que grabas, el teclado que haces en la computadora o pueden prender tu cámara y

grabarte, viene siendo más utilizado, pero no sólo viene siendo más utilizado en la región.

Entonces yo quería, antes de empezar, hablar sobre ello, quería darles a ustedes un ejemplo. Esto lo he tomado de un periódico americano, hice una pequeña traducción de un escenario de lo que ahora encontramos.

Y dice: “El adversario desarrolla algunas herramientas de Jaking en casa y compra otras del sector privado y puede activar, remotamente los micrófonos en los teléfonos”.

La nota continúa y, dice: “Después de desplegar el *Peilowt*, el adversario puede registrar las pulsaciones del teclado, leer correos electrónicos e incluso tomar foto de una cámara Web conectada por un período de 30 días”.

Sabemos que la mayoría de Malware o Software malicioso es criminal y se usa, sobre todo, para obtener información de sus cuentas bancarias, por ejemplo. Pero también lo utilizan para acceder a sus cuentas de correo electrónico o a sus contraseñas de redes sociales, que es el tema que nos convoca el día de hoy.

Ellos pueden obtener esa información, esa credencial para acceder a tus redes sociales, sea porque te envía un correo electrónico con un adjunto en el que tú haces clic y tu computadora queda infectada y con ello pueden tomar control remoto de ella, o sea porque haces clic en un Link, que era un Link falso que, como decía el expositor anterior, podía ser un banco ficticio que no era real y simplemente con esa información capturaban tu contraseña para acceder a tu cuenta bancaria y retirar todo el dinero o a veces es como una USB, por eso a veces yo no me separo de mi computadora porque uno se ve y con eso te instalan un Malware.

Entonces nosotros, en este ejemplo, yo puse ese ejemplo para ser, porque lo he hecho en otros lugares y les digo ¿quién es el adversario? Y todo el mundo dice: “El criminal que roba los bancos, anónimos algunos dicen”.

En realidad, en este caso fue, eso era lo del uso del Malware de manera criminal, pero en este caso fue el FBI. Hemos visto constantemente que no solo ya criminales o personas inescrupulosas, sino también aquellos que hacen cumplir la ley vienen utilizando estas herramientas de Jaking o de Cracking para infectar tus computadoras y eso resalta para una organización de la sociedad civil, una serie de preguntas: ¿Cuál es la autoridad legal que autoriza, las facultades legales que autorizan el uso de esas herramientas?

Y dos, ¿qué podemos hacer para proteger nuestra privacidad en línea cuando usamos las redes sociales, más allá de proteger, cambiar nuestra contraseña?

¿Y qué hemos visto? Recientemente, la semana pasada hay unos casos en el que varios activistas, muchos muy conocidos en nuestra organización, de todo el mundo, sean expertos en seguridad porque saben mucho de temas de tecnología y de seguridad, activistas de derechos humanos con un nombre reconocido, recibieron una notificación de Twitter, la red social de Microblogging y diciéndole que su cuenta había sido comprometida por un ataque de un estado.

No podían probar que efectivamente venía de un estado, pero que aconsejaban que, el mensaje decía, aquí está si lo quieren leer, está en inglés, y que aconsejaban qué implementen un mecanismo de seguridad y usen herramientas de anonimato en la red y recomendaban y ponían un enlace en nuestro propio manual de cómo protegerte en las redes sociales. Voy a hablar sobre eso al final de la conferencia.

Pero la idea de acá es que, y acá debemos agradecer a Twitter por haber notificado a los usuarios, porque los usuarios pudieron tomar una medida inmediata, que fue implementar un nivel de protección de dos factores.

¿Cómo funciona esto de dos factores? Lo cuento ahora porque es muy importante para el segundo caso que voy a mencionar.

Otro ataque contra la sociedad civil. Vimos que, parece, la organización canadiense, el Citizen Lab reveló que el Estado, no se sabe exactamente si fue el Estado de Irak o de Irán, es muy difícil

identificar el perpetrador, el adversario, había utilizado herramientas altamente especializadas para comprometer las cuentas Google Dox de activistas de derechos humanos.

Uno de esos activistas fue una persona que trabaja en mi organización, la Directora de Libertad de Expresión Jillian York y en el cual era una persona que se hacía pasar por un periodista de Routers, diciendo que necesitaba hablar con ella, comprobar su, es más la llamó desde un número teléfono de Reino Unido pidiéndole comprobar el número, la dirección de correo electrónico y él le enviaría material, que era un Link ficticio, a Google Dox, para lo cual ella tenía que confirmar la entrevista que Routers le iba a hacer.

El mensaje era erróneo, ella además trabaja en temas de Malware y está muy precavida de los temas.

Cometió un error, tenía una falta de ortografía en Routers, que por ahí uno sospechaba.

Y segundo, nosotros no hacemos clics en Link de personas extrañas que no conocemos.

Entonces dijo: No, dime por acá o envíame el mensaje en texto, pero no voy a hacer clic en un enlace.

Ella lo reenvió a los investigadores del Citizen Lab quienes hicieron toda esta revelación en medios y analizaron de dónde provenía.

El Email estaba enmascarado, no venía de Routers, venía de no sé sabe quién, de Irán pero no se sabe exactamente el estado, quién, pero que buscaba comprometer las cuentas de varios activistas que vivían en Estados Unidos y Canadá, haciendo trabajo para ellos.

Este sistema, que no voy a entrar a detalle, fue un esquema muy elaborado, porque primeramente atacaba el sistema de dos factores de autenticación.

Para explicarles un poquito qué es esto, les cuento brevemente. El sistema de autentificación funciona así, por ejemplo: Yo me conecto a

Google, me conecto a Twitter, voy a colocar mi password y recibo un mensaje de texto que va a mi teléfono, con un código.

Entonces una vez que recibo el código, voy a mi cuenta de Twitter o de Google, ingreso otra vez a clave pública y ahí ya estoy autenticada.

Para poder usar el sistema de dos factores que es muy recomendable para combatir el Malware, tú necesitas, primero, haber registrado tu teléfono en el sistema, en la red social.

Claro, esto es importante, ¿por qué? porque si alguien ha comprometido tu cuenta de Password de Google o de Twitter o de Facebook tú vas a recibir un mensaje y tú vas a saber que no te estás conectando a tu red. Eso quiere decir que alguien está comprometiendo su password.

Y por otro lado, aquellos que han comprometido tu password piensan que van a poder entrar a tu cuenta, pero no van a poder entrar a tu cuenta a menos que tengan tu teléfono. Claro que si pierdes tu teléfono, ahí sí ya estás en problemas.

Entonces, este ataque de los iranís era muy sofisticado, porque buscaba saltarse el sistema de dos factores de autenticación, pero el cual falló.

Nos alarma esto, Irán o Irak es muy lejos, me entiendes, no está en América Latina, pero hemos visto ya que la asociación reveló, en agosto del año pasado, que el gobierno ecuatoriano, especialmente el Servicio de Inteligencia, el SENAIN de Ecuador venía investigando a políticos, opositores políticos y también a periodistas.

Y ya sabemos, seguro muchos de ustedes se enteraron de las revelaciones de *Jakingtin*, esta empresa italiana dedicada a la comercialización de Software de espionaje que vende a estados.

Lo interesante de este Software de espionaje que también se conoce como “Galileo” o “Da Vinci” es un programa infecta tu computadora, como decíamos, permite sustraer datos, menajes, llamadas, correos electrónicos, ponerte un kiloware que permite que todas las teclas que presionan en tu teclado se vaya a esa persona, entre otras.

Vimos que ese Software se venía utilizando en varios países de la región, uno de ellos es en Ecuador con la Secretaría Nacional de Inteligencia, pero una investigación más reciente del Citizen Lab en noviembre, diciembre de este año reveló más, que además, que al parecer este Malware que proviene de estados, no estamos hablando ya de delincuentes, proviene de estados, venía siendo utilizando desde el Ecuador en otros tres países: Argentina y Venezuela y que fue utilizado para infectar el teléfono de uno de Nizman en Argentina, pero luego lo interesante de la investigación que se reveló por la Asociación el Citizen Lab en noviembre, es que encontraron que la información que recopilaba este Malware, tanto en Argentina, como en Ecuador y en Venezuela se enviaba al mismo Centro de Comando que al parecer provenía del Ecuador.

Claro, dicen países de izquierda. Ok, no estamos hablando solo de ello, hemos encontrado también y gracias a los Links de *Jakingtin*, que el gobierno mexicano es el comprador más grande de Malware de todos los clientes de *Jakingtin* en el mundo en términos de gasto e investigación.

Y más interesante aún, al menos desde el punto de vista legal, es que de todas las empresas o de todas las autoridades que tienen facultad legal para utilizar este sistema, como puede ser el CISEN, la Policía Federal, la PGR, la Fiscalía o procuradurías locales no eran sólo los únicos clientes, también lo compraron gobernantes de Baja California, Jalisco, Puebla Querétaro, Campeche, Durango, Estado de México, Tamaulipas que tienen facultad legal para espiar.

Nos preguntamos, además cuando nos enteramos, uno de los links decía que inclusive el Servicio de Inteligencia a su sistema de seguridad era inseguro. Salió esto publicado en la prensa.

Entonces ¿qué deb debemos hacer? Por un lado está el aspecto legal.

La pregunta es: ¿Cuál es la facultad legal que autoriza ese tipo de herramientas para investigaciones, que tal vez sí tienen un objetivo legítimo.

¿El juez está evaluando la proporcionalidad de la medida o está inclusive participando? ¿Es necesaria? ¿Es la medida más, no es la más, es la menos invasiva de todas las herramientas de vigilancia que existen? Son preguntas que yo no sé si el juez lo está evaluando.

Y por último, ¿existe una norma precisa que autorice su uso o simplemente están dando interpretaciones amplias de normas existentes, que con cláusulas como, y otros medios permiten legitimar cualquier tipo de vigilancia que invada la privacidad y la protección de datos de los usuarios sin tener en cuenta el nivel de proporcionalidad y necesidad? Estas son las preguntas que nos saltan desde el punto legal.

Ahora, desde el punto de vista técnico hay muchas cosas que podemos hacer, y para ello mi organización ha trabajado en una guía que se llama la "guía de autodefensa contra la protección, contra la vigilancia", la cual sirve para protegerte, sea contra un criminal o sea contra tu esposo porque tal vez no quieres que sepa todo o tu amante, no sé, o simplemente eres un profesor y quieres cubrir la información, quieres cubrir los exámenes para que no se revelen antes de tiempo, porque hay algunos alumnos muy hábiles con las computadoras.

Entonces, te enseñamos a cómo proteger esa información, que en verdad son normas aplicables a todo el mundo, no sólo el estado, también al estado, pero no es lo único y les recomendamos. Para protegerse del *malware* lamentablemente hay muy poco qué hacer, lo más importante es no hacer clic en *attachments*, en adjuntos.

Si alguien se los envía y no saben quién se los está enviando, mándenle un mensaje por un chat, llámenlo o por Facebook para preguntar si en verdad les están enviando el archivo, sólo para asegurar que no es un mensaje inseguro. Yo personalmente no cliqueo en *links* y pido que me envíen el mensaje en texto.

Recibí una invitación con una línea del gobierno brasileiro y un archivo adjunto, y no quise abrirlo, que era para una invitación muy grande de expositora, pero no estaba segura si eran ellos o no, así que los tuve que llamar para confirmar su email y luego me enviaron el mensaje en texto plano.

Ahora, a veces hay empresas como Google u otras empresas como Facebook y Twitter que están notificando a los usuarios cuando hay este tipo de medidas, sobre todo para enseñarles a que usen factores de doble autenticación, como les mencioné.

A veces hay *malwares* que son de acero, que son *malwares* en los cuales el antivirus no los va a capturar, porque la primera recomendación es actualizar tu antivirus, pero tal vez no lo pueda capturar porque son inéditos, todavía no se ha encontrado cómo curar el virus y para esos es mucho más difícil de protegerse.

Si alguna vez administras una red, tal vez monitoreando el tráfico te puedas dar cuenta que hay un tráfico inusual. Ahora, si estás infectado, te recomendamos desconectar la computadora y enviársela a un experto en seguridad, porque en verdad va a ser súper difícil; hay gente muy capacitada que sabe de estos temas, como acá en México el Rancho Electrónico, los chicos técnicos, la comunidad de *software* libre sabe sobre estos temas, pero hay que buscarlos.

Bueno, esas son las dos conclusiones, es un tema muy complejo, es un tema muy sensible, pero nuestra investigación en 13 países de la región ha notado, yo sólo mencioné dos o tres, ya no mencioné a Chile y a Argentina, porque simplemente no tenía media hora más para hablar de todos ellos, pero he encontrado el uso en muchos países y sin ningún tipo de debate público al respecto.

Entonces, me pareció una obligación de mi parte el poder compartir esos conocimientos con ustedes y provocar una discusión pública al respecto.

Gracias.

Com. Alejandro Torres Rogelio: Muchas gracias, Katitza.

Ahora en tu exposición me hiciste recordar cuando se promulgó la Ley Federal de Telecomunicaciones, que tiene disposiciones en las cuales diversas autoridades, ya no nada más la PGR o las que mencionaste, tienen facultades para intervenir comunicaciones, estas plataformas, conocer IPs y no sólo eso, sino obligar a las empresas a almacenar toda la información durante dos años, de todos.

Ahora cada vez que contratas uno de estos servicios las empresas deben guardar las empresa, seas o no sujeto de una investigación, te van guardando toda la información por si algún día se necesita. En mi opinión, es como si algún día vas a delinquir y vamos a utilizar todo tu historial, tu pasado, para demostrarte algo.

En el InfoDF intentamos combatir jurídicamente esa Ley, por lo menos esas disposiciones que contenían, un par de artículos, pero la Corte no nos reconoció el no tener facultades, atribuciones, porque éramos órgano garante local y eso le correspondía al órgano nacional, al INAI, que lamentablemente no lo hizo exactamente por el INAI.

Finalmente, permítanme nada más concluir el comentario. Es que yo creo que ninguna ley está escrita en piedra, si no se pudo combatir por la vía de la Corte, creo que ahora lo que quedaría sería una reforma por el Sistema Interamericano, correcto, pero también hacer una reforma de esa ley.

Vamos a dar ahora el uso de la palabra a Jesús Robles Maloof, quien es abogado por la Universidad Iberoamericana, maestro en Humanidades por la Universidad Autónoma Metropolitana. Tiene estudios de doctorado en Derechos Fundamentales por la Universidad Carlos Tercero de Madrid y doctorado en Humanidades por la Universidad Autónoma Metropolitana. Recibió la Medalla al Mérito Universitario 2008 por la misma universidad.

Fue educador en Derechos Humanos en la Comisión de Derechos Humanos del Distrito Federal, trabajó con personas en situación de calle en La Merced, fue Director Ejecutivo de la Academia Mexicana de Derechos Humanos y Presidente de Alternativa Social Demócrata en la Ciudad de México.

Es activista por el derecho de acceso a la justicia, el derecho a la privacidad de Internet libre, entre otros temas. Asesora a diversas organizaciones civiles en materia de estrategias de incidencia y libertad en Internet. Es integrante del colectivo de Activistas Digitales, Continente MX y es columnista en SinEmbargo MX.

En los últimos años ha colaborado recientemente con México Unido Contra la Delincuencia y Propuesta Cívica. Ha impartido conferencias sobre Derechos Humanos y actualmente colabora en *New Media Advocacy Project* en México.

Jesús, tienes el uso de la palabra por 15 minutos.

Muchas gracias.

Jesús Robles Maloof: Muchas gracias. Muy contento de estar aquí en la invitación del InfoDF.

Sí, es un día de celebración, creo que estos días tienen sentido cuando reflexionamos, cuando nos reunimos y la verdad estoy muy honrado en esta invitación.

¿Qué cosas podríamos celebrar? Para empezar, podemos celebrar que estamos aquí en un lugar significativo, me parece. Hace no menos de 40 años este lugar era una prisión, una prisión que precisamente intenta reflejar como quizá ninguna otra en el mundo, el panóptico de Jeremías Bentham.
Tengo amigos que estuvieron presos aquí, presos políticos. Se preguntarán amigos de qué edad, amigos ya grandes pero que luchaban por la libertad en este país y que estuvieron dentro de estas paredes. Y creo que eso, de entrada, hay que celebrarlo.

Segundo, creo que también tenemos que celebrar que existan instituciones y que tengan facultades a pesar de los embates contra la autonomía, a pesar de los embates contra la independencia, existen estas instituciones.

Y otra cosa que podríamos celebrar es que existe una sociedad civil internacional, como el caso que nos comentaba Katitza; existe también una sociedad civil nacional muy vigente, muy vibrante, como la que aquí está representada y existe una población que en la última encuesta, una encuesta que se hizo en 2014 en cuanto a la opinión sobre el tema de la vigilancia y la privacidad, en su mayoría se pronuncia en México contra la vigilancia y por la privacidad.

Creo que esos son temas que hay que celebrar, no creo que habría que “echarlos en saco roto”, a pesar de lo que a continuación voy a exponer, porque creo que también es importante decir los retos que tenemos, con todo respeto, como se usa siempre la muletilla antes de entrar a temas que quizá no son tan importantes, pero creo que es nuestro deber decirlo. No hay una sociedad ideal, la sociedad mexicana y las sociedades occidentales, por lo que yo conozco, no se asemejan a eso.

Voy a proponerles una hipótesis de reflexión. Me parece que la vigilancia se ha establecido como modelo de la política en México, en muchos otros países la vigilancia estatal, la vigilancia masiva y la vigilancia emerge desde el punto de vista del ciudadano como el mayor reto para la democracia, y voy a explicar por qué.

Cuando digo: El Mayo reto para la democracia, ya no son sólo las elecciones libres, ya no es sólo la libertad de expresión, me parece que el mayor reto actual es el estado de vigilancia y lo digo porque también ha avanzado.

Así como hice un recuento de las cosas positivas que hoy podríamos celebrar, me veo obligado a hacer, en honestidad intelectual, un recuento de las cosas que se han establecido sin que parezca que haya respuesta, respuesta de la sociedad y respuesta de las instituciones.

La primera es la simple idea que la vigilancia es necesaria. Casi nos han convencido que la vigilancia es necesaria y está justificada, y en muy pocas ocasiones pensamos: ¿Será necesaria? Es decir, antepone siempre el estado vigilante la hipótesis o el argumento de que es necesaria y por ahí vemos en las campañas electorales de esta ciudad, en las esquinas colgadas más cámaras para tener más vigilancia, más seguridad, dicen, ¿no? Entonces, uno se pone a pensar: ¿Será cierto?

La Ciudad de México cuenta con la segunda mayor infraestructura de vigilancia del mundo, sólo después de Londres. ¿Nos ha brindado más seguridad ese sistema de vigilancia multimillonario, que asciende a más de 16 mil millones de pesos anuales para esta ciudad? Estoy

hablando de esta ciudad. ¿Ustedes me podrían responder si ha dado más seguridad?

La semana pasada se presentó la estadística por el Consejo de Seguridad Pública del Distrito Federal, una entidad con colaboración oficial, que en la Ciudad de México han crecido 14 por ciento los homicidios.

Hay un estudio de la Universidad Autónoma Metropolitana que demuestra que las cámaras no han traído mayor seguridad y sólo en 10 casos probados, se los estoy diciendo, han servido como evidencia para atrapar a los responsables, 10 casos.

¿Ustedes invertirían, como en una empresa, 16 mil millones de pesos anuales para algo que no les trae mayor seguridad ni les ayuda a resolver crímenes? Les pregunto. Y pregunto: ¿Por qué no hay una oposición a esto? ¿Por qué no existe alguien que diga: “Oigan, vamos a detener esto, no tiene sentido”?

¿Hay alguien que dice: “Ya no vamos a destinar más dinero a esto”? Todo lo contrario, es: “Destinemos más dinero”. Ahora en el Metro de la ciudad, ¿quién vino en Metro de ustedes?, bueno, nuestros rostros quedaron grabados por el Sistema de Reconocimiento Facial del Metro de la ciudad.

¿Han visto el nuevo esquema de desarrollo del Programa Ciudad Segura? Unos travesaños que pasan a través de las principales avenidas, donde se dice que es de reconocimiento de placas, pero en realidad apuntan hacia enfrente. Ese sistema tiene capacidades de reconocimiento facial, porque las foto-multas, si han visto, son de toda la parte de atrás. ¿Por qué este nuevo sistema es de enfrente si sólo busca las placas? ¿No estaría bien que apuntaran hacia atrás?

Bueno, México, según la empresa Tales, que es una empresa militar francesa, va a convertirse en dos años, la Ciudad de México, en la ciudad con mayor inversión en vigilancia del mundo; no sólo a través de las cámaras, sino de sensores, multiplicidad de sensores y a través de la tecnología de reconocimiento facial.

Todo esto lo digo como un preámbulo para decir que toda esa inversión no tiene ningún sentido, ningún sentido para los objetivos formales, entonces, ¿para qué está? Nos preguntamos. ¿Toda esa inversión para qué se hizo? Toda esa inversión se hizo con otros motivos.

Muy rápido voy a desarrollar algunos argumentos un poco más relacionados con el tema que nos compete.

Como ya decía Katitza, México no sólo es el principal consumidor del *software HackingTeam* a nivel mundial, sino también de *Blue Coat,* que es otro software; el segundo consumidor mundial de *FinFisher* o *FinSpy* y en algunas mediciones está entre los primeros tres o cuatro consumidores de productos de vigilancia a nivel mundial.

Esto tuvo que ver con todo un crecimiento de los presupuestos de seguridad y, por ejemplo, el año pasado en una investigación que publicamos, México se convirtió en la principal sede de tecnología de vigilancia electrónica, de ferias de tecnología de vigilancia electrónica en el mundo y se realizaron cuatro ferias de la industria mundial, como en ningún otro país; las mayores ferias de la industria de vigilancia se realizan aquí, por lo que el título de investigación lo pueden leer en la página de Contingente MX, se llama: Las Pasarelas de la Vigilancia. Es decir, México se volvió una pasarela.

No sólo –como lo decía bien Katitza– el gobierno federal tiene amplios presupuestos sin control, sino también están los gobiernos estatales y los gobiernos municipales. El ex gobernador de Aguascalientes, Enrique Reynosa Femat, está siendo perseguido penalmente por dos delitos, el primero es por peculado y el segundo es por haber entregado *software* y *hardware* de vigilancia de alta tecnología al crimen organizado.

En Querétaro se encontró hace un mes, la nueva autoridad que llegó encontró una camioneta con tecnología IMSI-Catcher, que es una tecnología que usa técnicas de intercepción a la mitad; es decir, si mi celular se está conectando a la torre ponen una camioneta, captan la señal, decodifican la transmisión y reenvían la señal a la torre.

Entonces, el ayuntamiento, estoy hablando del ayuntamiento de Querétaro, dijo: ¿Y eso por qué está aquí? No sabemos, pero ahí la dejaron, el gobierno anterior ahí la dejó.

Estamos realizando una investigación en Cancún, en Quintana Roo, en el municipio de Benito Juárez y ha adquirido mayor tecnología que muchos gobiernos del mundo. El ayuntamiento de Benito Juárez ha adquirido mayor tecnología de vigilancia. ¿Para qué es esto, toda esta inversión millonaria?

Y un dato más, que lo quería decir hoy también, es que hemos la cuenta y hay un rubro nuevo en el presupuesto federal, desde 2014, que se llama: Operaciones Especiales y este rubro de Operaciones Especiales fue aprobado en 2014 con un monto aproximado de 25 mil millones de pesos, pues en 2015, hasta la última revisión que hicimos, que este presupuesto está para labores de inteligencia, de adquisición, de compra de servicios de vigilancia y de material, se había incrementado por encima de lo aprobado por el Congreso 700 por ciento. Es decir, habían gastado más de lo aprobado por el Congreso 700 veces.

¿Y saben qué particularidad tiene esta etiqueta en el presupuesto? Que no puede ser auditado. Operaciones Especiales tiene un código de reserva secreto. Por ahí decía un filósofo que en democracia lo que es secreto no cabe, pero así está, así es.

Quisiera entonces finalizar diciendo: ¿Todo esto para qué sirve? Todo esto sirve, no para darnos mayor seguridad, no es para la implementación del estado de derecho, todo esto sirve para vigilar. No es un asunto ajeno a nosotros que el lenguaje de la política en México es el espionaje, se hablan entre la clase política a través de escuchas, pero quizá hablan otro idioma diferente al de nosotros, por ejemplo, al Presidente del IFE le intervinieron su teléfono y es una manera de decir cosas, comunicarse cosas, y el Presidente sigue ahí, la denuncia que puso no llegó a ningún lado ni llegará a ningún lado.

¿Alguien me podría decir cuántas revelacionerevelaciones de escuchas, de correos, de conversaciones privadas han conocido en los últimos años? Casi cada semana conocemos una revelación, porque es el lenguaje de la política.

Primero, todo este dinero sirve, uno, para implementar un lenguaje político. Segundo, sirve para controlar a la disidencia. ¿Cuántos periodistas, defensores de Derechos Humanos, hemos sido intervenidos con alguna de estas tecnologías?

Y tiene otro factor que es todavía más terrible, desde mi punto de vista, para acabar esta escena un poco preocupante, que tiene un factor de inhibición en la democracia. Es decir, cuando nos sentimos vigilados no nos sentimos libres, no nos sentimos, vamos a decirlo así, en un ambiente propicio para la participación, para el debate.

Si sabemos que nuestro gobierno no nos va a revelar la información, si sabemos que tiene las capacidades de mantener secretos, el camino que se sigue es el camino del estado totalitario.

Yo así lo creo y por eso desde el 2014 estamos llevando una investigación sobre las capacidades de vigilancia del Estado mexicano, de todos los gobiernos y hemos ido documentando, tristemente, no a través de solicitudes de información, porque hemos realizado más de mil 500 solicitudes de información y sólo en un caso hemos tenido, a través de un recurso de revisión, acceso, si no, a través de filtraciones es como hemos llegado y a través de información cruzada, algo del trabajo de la Auditoría Superior de la Federación y algo del trabajo legislativo, pero casi no hay respuesta, hay muy poca investigación, los institutos hacen lo que pueden, por ejemplo, el InfoDF ha hecho algo sobre las cámaras en el Metrobús, pero falta mucho más acción y esa es la invitación el día de hoy.

Si queremos hoy salir con una tarea, es la tarea de preguntar, conocer, saber, por lo menos, para qué se usan y cómo se usan, porque les decía en Tlaxcala, en una conferencia que di, que les proponía que invirtieran 16 mil millones de pesos en poner estatuas mías en las esquinas y que les aseguraba que eso les iba a dar mayor seguridad, si ponían una estatua mía en cada esquina y los muchachos se reían, pero cuando presentamos en ese tiempo, que dio mucho más tiempo de analizar el efecto realmente que tienen las cámaras sobre la seguridad o la justicia, entendieron que es casi prácticamente lo mismo.

Estar invirtiendo en una democracia en eso, es estar básicamente otorgando carta blanca para que el Estado totalitario se consolide.

Quisiera terminar, entonces, diciendo –aunque normalmente cuando uno dice: "Yo quisiera terminar" se agarran otros 10 minutos– finalmente, que hay que involucrarnos un poco más y les dejaría, por supuesto, las direcciones del Contingente MX en Twitter, en redes sociales; Enjambre Digital, que es un proyecto del Contingente MX para la defensa de los derechos digitales y precisamente hemos implementado el litigio también en México para los casos que ya señalaba Katitza, que varios usuarios de Twitter en México han sido ya avisados por el mismo Twitter que algún gobierno, algún estado, ha estado sobre ellos y hacemos defensa legal de casos. Cuando conozcan un caso de censura, de intervención, con mucho gusto estaríamos dispuestos a involucrarnos.

Y desde el ámbito oficial, yo sé que muchos de ustedes son funcionarios, siempre pregunten: ¿Para qué es esta cámara? ¿Para qué funciona? ¿Para qué este protocolo de vigilancia? La clave yo creo que inicia con esa pregunta básica.

Muchas gracias.

Mtro. Alejandro Torres Rogelio: Muchas gracias, Jesús, nos pones a reflexionar. Interesa muchísimo esta información que das de mil 500 solicitudes y que sólo una tuvo éxito, y eso fue mediante recursos de revisión, no sé si fue hacia la instancia local o a la nacional, la federal; seguramente muchas de las solicitudes habrán sido de la instancia nacional y si habrán recurrido.

Creo que es ahí donde tenemos que probar a los órganos garantes también, no solamente en la cuestión de datos personales, sino también en el acceso a la información. Y ahora con el Sistema Nacional de Transparencia, que permite tener más una cuestión de revisión, los recursos de revisión locales ante la instancia nacional, utilizarla también y si no, ir al recurso de amparo. O sea, ir a todas las vías, creo, porque finalmente estamos hablando de derechos y de libertades, y con eso no se juega.

Pero también el tema que planteas respecto de las cámaras, más bien la percepción, pareciera que a la gente le gusta o más al gobierno le gusta más el tema de la percepción, que se sienta la gente segura, pero evidentemente una cámara no va a prevenir el delito.

No sé qué quisiera la gente con las cámaras, porque además, si revisáramos –que es algo que se me ocurre de momento– las solicitudes de información que pudiera haber en la ciudad, por ejemplo, respecto de las cámaras, la verdad es que mi percepción que es hay muchas solicitudes pidiendo la grabación de la cámara de la esquina tal y solamente que hubiera ahí alguna cuestión de una denuncia y las partes involucradas se tendría acceso a esa información y la gente no lo sabe; piden la grabación de esa cámara, pero realmente no se les da acceso, solamente a través de la vía jurisdiccional, el juez o el Ministerio Público pueden solicitar esa grabación.

Por otro lado, la Ley de Participación Ciudadana, como ustedes bien saben, la gente puede decidir respecto de proyectos para su colonia y muchos de esos proyectos tienen que ver con cuestiones de seguridad pública, particularmente cámaras, patrullas y la alarma del final. Eso es lo que piden.

Son temas interesantes que ahí están, pero finalmente sobre los que ha seguir trabajando para responder ésa y otras hipótesis que nos planteas.

Muchísimas gracias, Jesús, por tus planteamientos hoy.

Vamos a dar ahora el uso de la palabra a Jorge Flores Fernández. Él es Director y fundador de Pantallas Amigas. Es licenciado en Informática por la Universidad de Deusto. Su labor profesional se ha encaminado a la aplicación de la tecnología, al ámbito educativo.

En 2004 dedicó de manera exclusiva su trabajo a Pantallas Amigas, el desarrollo de guías y recursos didácticos como impresos, audiovisuales, material multimedia; también el asesoramiento o administraciones públicas, impartición de talleres y conferencias han sido parte de sus principales actividades en los campos de su especialización, como son el cyber-bullying, el cyber-acoso sexual a

menores, el *sexting*, las extorsiones, cyber-violencia de género, tecno adicciones y la cultura de la privacidad.

Jorge, bienvenido, muchísimas gracias.

Tienes el uso de la palabra.

Jorge Flores Fernández: Gracias por la presentación, en primer lugar. Agradecer sinceramente la oportunidad que nos ha dado InfoDF en la persona de su Comisionado Presidente, de la Comisionada Ciudadana, en este día de celebración, como dice Jesús, con ustedes y el elenco de expertos reconocidos que hemos podido ver hoy.

Les voy a pedir también, después de este agradecimiento, disculpas por adelantado, por una razón, simplemente porque hoy no soy la mejor versión de mí mismo. Llegué ayer muy tarde y mi compromiso era intentar aportar lo máximo posible, para eso uno viene de la organización, pero la verdad ando con flujos intermitentes de consciencia casi.

Entonces, me voy a apoyar en este pequeño guión para intentar no perderme demasiado y, como digo, cumplir de la mejor manera posible.

¿Por qué estamos aquí? No he venido de lejos, en concreto de Bilbao, luego Madrid, luego ya Aeroméxico hizo el resto, simplemente porque estábamos de alguna manera ya aquí. Nuestra actividad empezó en 2004 y desde entonces obviamente nació en un lugar determinado, pero siempre con vocación global.

Por dar algún dato, el número de visitantes en las páginas web que gestionamos, en un porcentaje altísimo, más allá del 25 por ciento, provienen de México; por dar un dato más concreto aun, en ese canal de Youtube que ha salido mencionado anteriormente, en el que en un día cualquiera, saben ustedes que varía obviamente, depende de cómo se haga la media y cómo transcurra, incluso cómo cambie el algoritmo, podemos recibir 50 mil videos al día, que se ven en nuestro canal, de personas de todo el mundo. De ese mundo, más allá, casi el 28 por ciento provienen de México.

Luego, venimos porque ya estábamos y sobre todo por la oportunidad que nos ha dado en este caso concreto INAI, que inició el ofrecimiento para traernos, para participar también la jornada de mañana.

¿Qué voy a intentar trasladar en estos menos de 15 minutos que tenemos? En primer lugar, una breve presentación, sobre todo para comunicar un poco en qué nos basamos y por qué lo hacemos así, y de esa manera poder entender cómo trabajamos en relación a la privacidad.

En segundo lugar, por qué si hablamos de menores, de seguridad, por qué ese énfasis específico en privacidad, que creo que nos diferencia de otras organizaciones.

En tercer lugar, cómo pensamos que está la sociedad en general abordando esta cuestión, en concreto los chavos y las chavas.

Y en cuarto lugar, en qué pensamos que tiene que cambiar un poco, que incidir más.

Y terminaré dando algunos ejemplos de proyectos que hemos hecho y cuál es su fundamentación, y en ese caso también su utilidad, que están ahí a disposición de ustedes en su mayor parte en la página web.

Pantallas Amigas nace en 2004 con un único objetivo en aquél entonces, promoción del uso seguro y saludable, de nuevo la salud, estamos hablando de 2004, de las tecnologías, hablábamos de Internet, celulares, por aquél entonces, sin acceso a Internet en su mayor parte y videojuegos, por parte de la infancia y la adolescencia.

Ese fue nuestro único reto y sí que, aunque partimos de 2004 con cero experiencia, sí que nos apoyamos en 30 años de trabajo previo, de una organización que se llama EDEX, que llevaba ya, como digo, 30 años trabajando en la infancia y la adolescencia. Tomamos todo ese *background* y lo incorporamos a ese trabajo, que en ese momento comenzaba.

Ése fue nuestro inicio. Posteriormente, en 2009, incorporamos un segundo lema, que era: Por una Ciudadanía Digital Responsable.

Sabíamos que eso había que abordarlo desde mucho antes, pero entendíamos que la sociedad no estaba preparada para ese mensaje, no estaba más preocupada de la seguridad que de la ciudadanía digital. Tuvimos que esperar a 2009 para incorporarlo como un segundo lema.

Nuestro enfoque respecto de tecnologías e infancia es positivo, aunque nos toque hablar de riesgos y no nos importa, porque los asumimos con naturalidad, como hay riesgos en el tránsito, no pasa nada por hablar de accidentes de tránsito, nadie criminaliza a los autos. Esa etapa la hemos pasado.

Hablamos en un sentido amplio de la tecnología no sólo como a veces se aborda, para proteger a la infancia, no, hablamos en un sentido amplio de promoción de la infancia, de protección y también de participación. Esos tres aspectos son en los que podríamos clasificar los 51 artículos de la Convención de los Derechos de la Infancia. Nuestra visión es más amplia y, en este caso, por eso el lazo, hablamos de privacidad como derecho, en primer lugar.

¿Cómo lo abordamos? ¿Cómo hacemos nuestro trabajo? ¿Cuáles son nuestros pilares? Desde el principio y no los hemos movido un ápice, y han pasado casi 12 años, en primer lugar, comunicación educativa; no podemos ir a los más pequeños con mensajes escritos, su lenguaje es audiovisual, lo comentaba Lina, cuando buscaba un contenido concreto lo hacía en Youtube, su dieta digital es audiovisual y no nos podemos dirigir a ellos de otra manera.

En segundo lugar tenemos en cuenta transversalidad con estos aspectos educativos. Podemos hablar de prevención de riesgos, pero es que tenemos plenamente consciente que hay que tomar cuestiones como la equidad de género cuando abordemos ese tipo de problemas, es decir, reflejarlo de una manera o de otra, y si hacemos renuncias, que sean conscientes. Estamos hablando de educar de forma integral, no podemos trabajar en un aspecto y tumbar otros.

En tercer lugar, probamos cosas, nos encanta probar cosas, son arriesgadas, nos cuesta mucho trabajo, pero si el mundo ha cambiado tanto, ¿qué hacemos haciendo lo mismo? En ese sentido, podemos decir que hemos innovado en numerosas ocasiones.

Hablamos también de valores, es importante, no tratamos de adoctrinar a nadie, pero creo que hay valores universales que todos y todas compartimos, y los tratamos también de reflejar.

Por último y muy importante, más importante cada vez, yo creo, las habilidades para la vida definidas por la OMS creo que fue en 1993 y que son aquellas que nos permiten desarrollarnos de forma plena y saludable, teniendo en cuenta que salud no es ausencia de enfermedad, sino pleno bienestar físico, emocional y social.

Eso es lo que guía de alguna forma todo nuestro trabajo y cómo vamos a llegar a donde finalmente pondremos algunos ejemplos.

¿Por qué la privacidad? Lo he comentado, es un derecho de las personas, la ONU lo ha reconocido incluso más recientemente y si vamos a la Convención de los Derechos del Niño, y relacionado con Internet, creo que no estamos tomando muy en cuenta el interés superior del menor, reconocido por la Convención, a la hora de tomar decisiones.

Desde todos puntos de vista porque es un derecho, pero también y muy importante, porque es un factor de protección. Hablamos y no les importa hablar de proteger, y frente a la violencia digital, que es sobre todo muy fácil de realizar y muy asimétrica entre el que victimiza y la víctima, creo que es muy importante preservar todos los factores de protección o de salvaguarda de la víctima, y la privacidad es uno de ellos fundamental. Por eso hacemos especial énfasis en ese aspecto.

¿Cómo se está trabajando actualmente? Creo que el mensaje no ha evolucionado mucho. Se habla en algunos casos de tu reputación digital, “fíjate cuando vayas a encontrar un trabajo”, hombre, es cierto, pero estamos en contacto permanente con los y las adolescentes, y me cuesta pensar que un chavo de 14 años vaya a publicar o no una cosa en Instagram pensando en el trabajo de su futuro, me cuesta. Y se repite permanentemente, pero la verdad no lo veo claro.

Por otro lado también se dice: “Configura tus opciones de privacidad”, de acuerdo, es lo que tú puedes hacer, perfecto. Sin embargo, creo que lo que no se está haciendo, por supuesto también hay

organizaciones de la sociedad civil que tratan de intervenir en la regulación y la autorregulación de las empresas, y eso es importantísimo, pero creo que hay un aspecto que no se está cuidando lo suficiente, y es lo que me atrevo a llamar, que no sé si existe la palabra, pero 13 horas de avión dan para mucho, la coprivacidad.

La coprivacidad como privacidad entendida en corresponsabilidad, en una sociedad híper conectada, que va rápido, que va fluida, que no da tiempo a pensar y cuando relaciono esto con privacidad, ¿qué quiero decir? Se habla mucho y he puesto ejemplos, de lo que uno publica, lo que uno tiene que hacer con la red social para que esa red social no publique muchas cosas, es decir, configurar las opciones de privacidad; pero se habla muy poco, creo, del tercer factor, que es lo que las otras personas pueden publicar de ti y ese es, por supuesto, el mayor riesgo, por desgracia.

Uno puede controlar una cosa, la red social puede hacer o no lo que pensamos que vaya a hacer, pero lo que más nos cuesta controlar o gestionar es a otras personas que comparten nuestra vida a golpe de clic. Nadie se plante a la hora de enviar una información o una imagen si esa otra persona tiene los mismos valores que tú a la hora que se tiene que compartir o no, si tiene las mismas competencias que tú o no, o las competencias necesarias para proteger esa información, pensemos en un novio y una novia que se mandan fotos íntimas, para proteger de forma normal y natural esa información o esas habilidades para gestionarla, nadie nos lo planteamos y en eso estamos todos y todas comprometidos.

¿De qué me sirve que yo cuide muy bien mi privacidad si comparto datos con mi compañero que también sufrió las 13 horas de avión y él no tiene los mismos criterios que yo, es descuidado, se deja las cosas por ahí? ¿De qué sirve? Respecto de la privacidad y la cyber-seguridad, creo que falta un empuje muy importante de consciencia colectiva.

Uno hace lo que puede hacer, sí, pero si el de al lado, con quien te relacionas, no lo hace, estás igualmente perdido. Creo que en ese mensaje hay que incidir mucho.

Por ir cerrando un poco el círculo y no extenderme mucho aquí. Por ejemplo, las etiquetas en las redes sociales, es un tema que abordamos hace muchísimo tiempo y es un tema para plantear, con qué derecho alguien en una foto que pretendidamente es anónima, aunque uno salga ahí, pero en la red se puede perder entre muchas fotos, aunque le autoriza o se lo permita la red social, dice que ese conjunto de puntitos soy yo y me identifica con mi nombre, me da una identidad; además, ya se va a encargar la red social de difundir que yo salgo en esa imagen, aparte, con todo lo que significa esa imagen, que estoy con quién, dónde, en qué momento y de qué manera. En las etiquetas de las redes sociales nadie "ha levantado la liebre" y me parece un caso muy evidente de coprivacidad.

Hace ya tiempo lo planteamos a dos redes sociales, en este caso en España, una hizo oídos sordos y la otra, la verdad, el abogado responsable de la privacidad se quedó un poco en plan positivo, recibió el mensaje, se quedo reflexivo y dijo: "Desde Europa no nos están diciendo nada sobre esto y hoy te estás planteando si es hasta legal", pues la verdad es que ahí quedó.

Las etiquetas son una invasión bestial de la privacidad y además están siendo utilizadas para el cyber-hostigamiento, eso está claro. ¿Qué menos que solicitar un consentimiento previo y expreso de la persona afectada cuando alguien te va a publicar o te va a identificar en una fotografía? ¿Qué menos? Eso no cuesta nada.

Los que saben algo de códigos, sabrán que son tres líneas de código, cuatro a lo sumo y no lo hacen porque no les interesa. De hecho, este abogado que me devolvió en positivo la respuesta, me dijo: "Mira, tienes toda la razón pero no nos dan los números", es decir, su negocio no lo permitía. También yo me planteo si realmente se pierde el negocio en limitar esa cuestión.

Podría llegar a ser legal, porque uno acepta las condiciones generales de la red social, si nos lo ponen ahí, podría ser más o menos engañosa la manera en que nos lo plantean, ¿pero es ético con los menores? ¿Es ético en general? Habría que planteárselo. Ese es un ejemplo de coprivacidad.

Por poner tres casos de cómo hemos venido trabajando a lo largo de este tiempo cuestiones relativas al fomento de la cultura de la privacidad entre las y los menores de edad, hicimos hace ya mucho tiempo un proyecto que, efectivamente, se llamaba: Etiqueta sin Problemas y simplemente reflejaba en varias historias animadas, lenguaje audiovisual, diferentes situaciones en las que se causaba daño a otra persona de forma consciente o incluso inconsciente, que eso es lo grave; etiquetasinproblemas.com y están todos accesibles desde nuestra página web pantallasamigas.net, por eso no me voy a extender ahí.

Ese es un ejemplo de cómo lo trabajamos. Otro ejemplo fue un proyecto que desarrollamos con la agencia básica de protección de datos, que se llamaba Reda y Neto, que eran los dos protagonistas, y abordábamos ya la cultura de la privacidad desde los ocho, nueve años de edad; pero es que no les decíamos qué pasará con tus fotos cuando sean mayores, lo que les decíamos principalmente era que intentábamos que dieran valor a sus datos personales desde temprana edad.

Yo no sé si lo llegaron a razonar o no, pero que les llegara ese concepto que tus datos personales valen y son utilizados en la red en la que tú vives como moneda de cambio, es un mensaje importantísimo. Diseñamos esas animaciones para animar el debate y también actividades didácticas para desarrollar no sólo en el centro educativo, sino también en la familia, por aquello que tiene de importancia la influencia próxima y ese es otro ejemplo que está en la red, por dónde vamos y por dónde confluye todo lo que les he contado a ustedes.

El último, más en sentido amplio, se llamaba netiquetate.com, que no tiene que ver con etiquetas, sino con la netiqueta o código de buenas prácticas, de buena conducta o hábitos sociales en las redes. En esa netiqueta muchas de las reglas que proponíamos, aunque luego las volcábamos a revisión por los y las protagonistas, que son los propios adolescentes, para que sobre ese previo las cambiaran, son ellos quienes hacen las reglas de su comunidad, y eso era parte del mensaje, pero no interveníamos mucho en la privacidad.

Cuando, por ejemplo, Daniel y se lo he comentado al salir, hablaba de respetar a los demás, nos decía en su conferencia, que hablaba del cyber-acoso, pero no se detuvo en hablar de respeto a la privacidad de los demás; es decir, no hacer daño invadiendo su privacidad o ser respetuoso con la privacidad. Este tipo de mensajes son importantes, como también la responsabilidad que cada cual tiene respecto a la información de los demás.

El concepto de ciudadanía digital supone, en definitiva, el ejercicio consciente y efectivo de derechos y deberes. Ya ahí estamos en una ciudadanía digital que se está reinventando a cada paso, que va muy rápido y que pone a nuestro alcance herramientas cada vez más potentes, pero más etéreas en algunos sentidos, más ocultas.

En definitiva, y este era un poco el mensaje, en una sociedad hiperconectada qué es lo que debemos tener en cuenta, la ciudadanía digital y abundar en el enfoque de corresponsabilidad, y de alguna manera coprivacidad.

Gracias.

Mtro. Alejandro Torres Rogelio: Muchas gracias. Interesante el concepto que nos planteas, pero sobre todo creo que el trabajo de Pantallas Amigas apunta a lo que considero fundamental, la seguridad empieza por uno mismo, así que cuando uno se anda sorprendiendo que le llaman a su teléfono celular, le hablan por su nombre para ofrecerle equis producto, un banco o lo que sea, uno se anda espantando de por qué sus datos andan por ahí, pero la verdad es que en la vida cotidiana andamos regalando nuestros datos por ahí, así, sin el mayor cuidado, no tenemos consciencia de lo que estamos haciendo.

El trabajo de Pantallas Amigas creo que también apunta mucho a esa educación digital que debemos hacer, que además tiene un gran valor, se enfoca a un sector que nos cuesta mucho trabajo, sobre todo nuestros hijos, nuestras familias. Así que creo que hay que agradecer muchísimo a Pantallas Amigas por el trabajo que realizan, porque nos lo facilita muchísimo.

Quisiera preguntarles: ¿Quién ha visto el trabajo de Pantallas Amigas? Si pudieran levantar las manos. Uno y es del Info, supongo que por cuestión de trabajo. Quiero que sepan qué es Pantallas Amigas, que está haciendo esa labor y que nos puede ayudar muchísimo en esa educación digital, tanto de nuestros hijos como de nosotros mismos, también ayuda muchísimo. Uno debe revisar el trabajo de Pantallas Amigas.

Luego, lo que ha dicho también respecto del valor de la información, claro, la economía es "la mano que mece la cuna" en todo esto, en buena medida, así que cuando a uno le dicen cuando va a comprar algo, por ejemplo, a una cadena de farmacias que hay aquí, que ofrecen una tarjeta de lealtad y no sé qué otros títulos le ponen, que por cada compra le abonan a uno un porcentaje, equis cantidad o puntos, la verdad es que no le están a uno regalando nada, le están comprando la información y además uno está malbaratando la información, y es información muy sensible la que en muchas ocasiones damos, no de manera consciente.

Entonces, creo que debemos tener cuidado, sobre todo en esta parte del auto cuidado, la educación, la seguridad empieza por uno mismo y en eso interviene mucho la educación, que es el trabajo que en buena medida hace Pantallas Amigas.

Muchísimas gracias, Jorge, por compartir tu experiencia y conocimientos con ello, y por el esfuerzo físico también que haces con ello también, no es fácil, lo sabemos. Como se dice aquí, vienes "en vivo" casi.

Vamos a dar ahora la palabra a Carlos Martínez Velázquez, quien es politólogo por el Instituto Tecnológico Autónomo de México, el ITAM. Actualmente dirige los trabajos de Central Ciudadano y Consumidor, que es una organización civil dedicada a temas de consumo, regulación y competencia económica.

Ha trabajado antes en distintas áreas gubernamentales, como la oficina de la Presidencia de la República, la Secretaría de Economía y la Procuraduría Federal del Consumidor.

Sus temas de investigación son: Regulación económica, desarrollo, desigualdad, gobierno abierto, participación ciudadana y derechos del consumidor.

Ha sido investigador del Centro de Estudios sobre Impunidad y Justicia de la Universidad de Las Américas, Puebla. Es columnista y participante en distintos medios de comunicación y actual consejero editorial de la sección Negocios del Grupo Reforma.

Por favor, Carlos.

Carlos Martínez Velázquez: Muchas gracias. Agradezco la invitación al InfoDF, ya es el segundo año en que estamos, desde hace un año no veía a Katitza y ahora me encuentro con Jesús, que hace también muchos años que no lo veía. Entonces, está muy bien estar en esta serie de conferencias para reflexionar sobre la protección de datos.

Ya veíamos lo que hablaban antes, el tema del Estado, el tema, por supuesto, de la corresponsabilidad en protección de datos y la privacidad de las personas, y precisamente ahora el Comisionado hablaba de la parte económica, que eso es algo de lo que hacemos en la organización, investigación económica, de competencia, regulatoria, internacional y por eso yo había pensado en centrarme justamente en esto.

Veía hace poco un estudio de Global, que es una empresa EMC, donde le preguntaban a los usuarios de Internet cuál era su disposición a dar datos, dado que obtenían a cambio una mayor usabilidad de la red.

Entonces, encuesta a 15 países, entre ellos México y México es de los países donde el 43 por ciento de las personas están dispuestas a dar sus datos por tener mucho mayor conveniencia y uso de los portales de Internet, comparado con el 27 por ciento, que era el promedio de todos los demás países.

¿Esto qué nos dice? Que hay un asunto económico atrás de dar datos. Los datos, de hecho, son el lubricante del Internet; el Internet funciona gracias a los datos y precisamente los datos personales

ayudan a hacer mucho más fácil encuentros entre personas, a hacer mucho más fácil el intercambio de productos de consumo y demás.

Así que llegamos a un punto donde los datos personales se dividen generalmente para el estudio entre los datos que se dan para el comercio electrónico y los datos que se dan dentro de las redes sociales, pero conforme avance el Internet vemos que hay una unión entre el comercio electrónico y las propias redes sociales.

Nuevos esquemas económicos, como UBER, RB&B, etcétera, son a la vez una red social, porque son empresas que generan efectos de red en la economía y que se basan en el intercambio de uno a uno, y a la vez son intercambio de servicios que tienen un valor económico.

Esto nos habla de cómo se está juntando el tema de las redes sociales y el comercio electrónico, y hacia allá va el futuro del Internet, pero eso también nos habla de cuánto valen los datos.

Ya lo decía Jorge, los datos tienen un valor importantísimo en la red y precisamente eso sirve para hacer mucho más fáciles las cosas, y los internautas enfrentamos varios dilemas. El dilema es: Si esto hace más fácil el Internet, ¿por qué no voy a dar mis datos personales?

Entonces, tenemos tres paradojas que atender. Queremos que el Internet funcione padrísimo, que nos den nuestras ofertas personalizadas, etcétera, pero no queremos dar ningún dato personal. Bueno, esa es una clara paradoja, porque no puedes negar dar los datos y a la vez querer que te personalicen todo en el Internet.

Luego tienes otra, que es no tomar ninguna acción. Sabes de los riesgos de dar tus datos personales, pero no tomas ninguna acción, ni en lo personal, o sea, dices: “Bueno, ya, doy mis datos, así funcionan las cosas” y no hago nada.

Y, por otro lado, tienes gente que valora muchísimo su privacidad, que dice: “Me encanta proteger mi privacidad”, pero comparten cantidades ingentes de datos en Facebook, se la pasan subiendo la foto del niño, del sobrino, de la boda y todo el tiempo. Entonces, comparten muchísimo, aunque tienen la consciencia sobre los datos personales.

Enfrentamos esas paradojas sobre cómo compartir y qué compartir en la red, y esto genera la siguiente pregunta: ¿Quién se tiene que encargar de resolver esta serie de paradojas? Y la respuesta obvia es, el Estado; pero el Estado está compuesto por las propias empresas, por la sociedad civil y en general por los gobiernos.

Entre ellos tres tienen que garantizar esta protección a la privacidad, porque finalmente el individuo, que es la forma más pequeña del Estado, es la esfera máxima de la privacidad, el individuo es en sí mismo el que tiene esos derechos a la privacidad y además a quien le tienes que proteger frente a toda la colectividad.

El Estado tiene esto y las empresas son corresponsables también de la protección de los datos, por eso se generan las leyes como la Ley de Protección de Datos en Posesión de Particulares, etcétera, y hacia allá vamos viendo cómo avanza la parte internacional.

Hoy que se está discutiendo el Tratado Transpacífico, por ejemplo, o en el caso de la Unión Europea el Tratado entre Europa y Estados Unidos en materia de Comercio, hay capítulos específicos sobre el tema de datos personales y el tema de comercio electrónico, de hecho, en Europa mucha de la discusión sobre la protección de datos se ha dado a través del comercio, estuvo el caso del *safe harbor* en la Unión Europea en el año 2000 y ahí era un intercambio de cómo las empresas de Estados Unidos ofrecían servicios en Europa y obtenían datos de ciudadanos europeos, entonces había un sistema de resolución de disputas entre Estados Unidos y la Unión Europea, y había sistemas para que los usuarios pudieran garantizar la protección.

Finalmente, el Tribunal Europeo recientemente dijo que el puerto seguro no es un mecanismo válido para el intercambio de datos entre el continente europeo y Estados Unidos, y esto afecta distintas áreas del comercio y demás. Pero creo que los tratados comerciales son una gran oportunidad, porque más allá de cuestiones específicas sobre cómo se construyen y la participación que no tienen, y demás, creo que tenemos que verlos como una oportunidad para discutir cómo se intercambian los datos personales en una economía global y en una economía interconectada que están generando empresas que no son sujetas de los marcos nacionales y que a lo mejor una empresa china

me está vendiendo a mí, tiene mis datos, se rige por la regulación china, etcétera.

Entonces, hay que pensar en cómo la economía y este intercambio genera o debe generar una consciencia sobre los datos personales. Y en ese sentido hay que pensar nada más cómo estamos en México.

México, en términos de comercio electrónico, es muy incipiente, de hecho, los mexicanos no confiamos en el comercio electrónico y no confiamos porque pensamos, uno, que por supuesto nos van a robar vuestro nuestro dinero, porque damos datos altamente sensibles como tarjetas de crédito.

Otro, no confiamos en las empresas, tenemos muy mala experiencia como consumidores en general y pensamos que, uno, nos van a dar "gato por liebre" o no nos va a llegar el producto que pidamos, etcétera. Entonces, usamos el Internet como una forma de buscar los productos, pero siempre vamos a comprarlos a la tienda.

En general, los latinoamericanos somos un poco desconfiados en el tema del comercio electrónico, sin embargo, en México el cinco por ciento del total de las ventas minoristas se dan a través de Internet. Lo que significa ahora el Tratado Transpacífico es el 21 por ciento del comercio *retail* que va a ser en Internet y son empresas que van a estar en otros lados y que tenemos que pensar que ellos van a ser parte de nuestros datos.

AMIPCI sacaba hace poco un estudio sobre datos personales y le preguntaba a los internautas mexicanos cuáles eran sus actitudes frente a la privacidad, nueve de cada 10 han dado datos personales, 6 por ciento han habilitado las opciones de privacidad y según ellos pican el botón y dice: "Sesión privada" o no sé qué, pero el 61 por ciento no saben cómo operan esos términos de privacidad.

O sea, en realidad estamos siguiendo una serie de cosas que a lo mejor muchos se dedican, muchos de la sociedad civil nos dedicamos precisamente a simplificar y a entender que tienes que apretar tal botón, que tienen tales datos y tal pero, por otro lado, hay una falta de internalización de los ciudadanos, de los consumidores, en cómo operan estas partes de datos. Y 32 por ciento se consideran que no

tienen control sobre sus datos, imagínense que un tercio de la gente que utiliza Internet en México piensa que no tiene control sobre sus datos y es gravísimo, porque ellos son los titulares de los datos.

¿Cuál tendría que ser la solución para esto? Por supuesto la corresponsabilidad entre el Estado y las empresas pero, por otro lado, se tienen que establecer estándares y directrices que protejan a los usuarios y los consumidores, que tienen que ser muy claras y tienen que ser, sobre todo, operables, porque aquí en México siempre nos encanta poner unas leyes padrísimas que son inoperables o que no se pueden castigar.

Tienen que haber mecanismos claros de compensación a los usuarios, cada vez que ellos reclaman que haya baja de sus datos, etcétera, tiene que haber mecanismos de compensación claros y eficientes para los consumidores, porque también meterlos en un asunto burocrático sin fin, te desanima a reclamar temas de mal uso de los datos personales. Y en la medida en que las instancias gubernamentales se fortalezcan ahí, es mucho más fácil establecer el tema con las empresas, por supuesto.

Procedimientos claros para la reclamación de los datos, castigos fuertes para fraudes y robo de identidad, que eso es algo que sucede todos los días, no sólo es que te roben los datos de tu tarjeta de crédito y utilicen mal tu dinero, también es suplantación de identidad y demás, que genera una serie de problemas en la esfera ya *offline* y que nosotros debemos tener mecanismos de defensa ante estos robos, que muchas veces no nos damos cuenta hasta que sucede que alguien cometió un delito con nuestra identidad en línea.

Así que debemos tener muy claro qué es esto, pero el Estado también debe garantizar de una manera eficiente, fuerte, de castigar este tipo de delitos. Y lo otro es avanzar hacia temas de autorregulación vinculante con las empresas, que eso es algo que precisamente la última versión de la Ley Federal de Protección de Datos Personales en Posesión de Particulares establece, un capítulo de autorregulación vinculante, y esto es bien importante, porque sí, el Estado, el gobierno como parte del Estado, es el que tiene que perseguir, castigar y compensar.

En este sentido, funciona como un agente compensador en este entramado, pero las empresas son las que finalmente operan los datos, los pueden vender, pueden hacer operaciones con ellos y demás. Entonces, tiene que haber un mecanismo de corresponsabilidad en tramos actores, de lo contrario, te vuelves un Estado que se vuelve hipervigilante, que es lo que ya decíamos con este asunto de la seguridad y empresas que no se comprometen con los usuarios y con los consumidores a proteger nada, porque también ellos combaten o son clientes del estado vigilante.

Tenemos que romper esto haciéndonos responsables todos de la privacidad y de la protección de datos personales.

Hasta aquí dejaría este entramado y esta reflexión de cómo tenemos que juntar y pensar, cuando pensamos en Internet, tanto en la parte comercial como en la parte de redes sociales, etcétera, porque finalmente todo confluye hacia nuestra participación en línea frente a los estados, las empresas y demás.

Muchas gracias.

Mtro. Alejandro Torres Rogelio: Muchas gracias, Carlos.

Hace poco, a finales de octubre, se realizó la Conferencia Internacional de Comisionados de Protección de Datos Personales en Ámsterdam y ahí el documento base de trabajo fue el que se tituló como: Construyendo Puentes, que básicamente es construir puentes entre europeos y americanos, que son los que traen el gran debate y la gran pelea por la cuestión de los datos personales.

Pero ello tiene una grave implicación para nosotros, porque resulta que Estados Unidos es nuestro principal socio comercial. Entonces, cuando nosotros tengamos que definir los términos de una Ley Genera del Protección de Datos Personales, con la cual se va a armonizar la Ley Federal y las leyes locales, tanto para los datos personales que estén en instituciones públicas como en los privados, finalmente es el mismo derecho el que se ejerce entre ambas instancias, públicas y privadas, tenemos que definir entonces cuál es nuestra postura, porque ello va a implicar una cuestión más restrictiva y más

reguladora, como es la europea o una más abierta, que es la americana.

¿Cuál es el modelo que vamos a definir? Porque de ello depende también nuestra economía y la economía digital está creciendo muchísimo.

Es un gran debate sobre el cual no deberíamos perder, que además ya vamos tarde, porque tú lo mencionaste de manera tangencial, pero ahora está el Acuerdo de Asociación Transpacífico, el TPP, donde tiene una gran implicación precisamente el comercio de datos, finalmente y lo que está en el fondo no es la cuestión económica, es la seguridad de las personas, es la integridad de las personas, es el debate.

Muchísimas gracias por poner estos puntos, este enfoque, hoy en este panel.

Vamos ahora a dar el uso de la palabra a Paulina Gutiérrez, quien es Oficial Adjunto del Programa Legal de Artículo 19, Oficina para México y Centroamérica. Ella está a cargo de la estrategia digital y el análisis jurídico de la regulación de Internet. Coordina la estrategia de género y las acciones ante mecanismos internacionales en el Sistema Interamericano de Derechos Humanos y de Naciones Unidas.

Es abogada y licenciada en Relaciones Internacionales por el Instituto Tecnológico de Estudios Superiores de Occidente, el ITESO. Cuenta con 10 años de experiencia en materia de defensa, protección y promoción de los derechos humanos, tanto en el ámbito nacional como internacional.

Tiene una estancia en la Comisión Interamericana de Derechos Humanos y ha realizado investigaciones sobre migración temporal, tortura, seguridad humana y seguridad ciudadana.

También ha colaborado en proyectos de litigio estratégico, ha dado acompañamiento integral a víctimas de violaciones graves a los Derechos Humanos y coordinado la capacitación de funcionarios, jueces y cuerpos de seguridad pública en materia de Derechos Humanos.

Muchísimas gracias por acompañarnos hoy. Tienes el uso de la palabra.

Paulina Gutiérrez: Muchísimas gracias a usted.

Yo quiero iniciar tal cual agradeciendo que se abra el espacio, entiendo que no es la primera vez de este espacio en donde se abre a la sociedad civil para discutir temas de Internet. Justo también en los foros internacionales se ha considerado como una de las mejores prácticas para intentar tal cual estandarizar la protección de los derechos de todas las personas que estamos usando el Internet hoy en día.

Así que agradecer también este espacio y ahora sí que invitar a que no se cierren en ningún momento, a pesar de las muchas opiniones encontradas que podríamos tener la sociedad civil con respecto al funcionamiento que está teniendo el Estado en temas como los que ya se plantearon en este momento, como lo es la vigilancia que en algún momento creo que podré retomar algo de lo que ya dijeron Jesús y Katitza, para justo explicar un poco por qué desde Artículo 19 vemos con preocupación que no se logre conectar con mucha fortaleza la defensa del derecho a la libertad de expresión, vinculada directamente con la privacidad, que implica también los datos personales.

Es decir, los datos personales, vistos de manera aislada, pueden incluso fomentar, o sea, una protección desde los organismos grandes pueden incluso fomentar una limitación al flujo de información, porque muchas veces las excepciones que hay también a la protección de datos personales están vinculados a la libertad de expresión y esto sucede en las redes sociales.

O sea, en las redes sociales nos hemos dado cuenta, a pesar de los escenarios terribles que podemos llegar a plantear desde la sociedad civil que también son estos espacios y plataformas donde intercambiamos información de manera masiva, y que tiene que ver con espacios que antes no existían para hablar de temas de corrupción, temas de interés público, manejo de presupuesto, etcétera.

Estas plataformas han sido determinantes para que esta información sea difundida y accedida por toda la sociedad. Entonces, este tipo de información es, como lo han mencionado Jesús y Katitza, mientras existan las medidas de vigilancia y mientras haya una regulación a esta vigilancia, por mucho que no se pueda justificar su necesidad y su proporcionalidad, no da confianza a los usuarios de las redes sociales, y esto tiene un impacto directo en la libertad de expresión. ¿Por qué? porque nos limitamos a compartir información que puede considerarse de interés público.

En esa medida, yo quisiera retomar un poco lo que hablaron sobre la Ley Telecom. La Vigilancia como tal, a pesar que está comprobado que la vigilancia secreta ya dejó de ser secreta, creo que todos sabemos perfectamente qué medidas están, las conocemos las empresas, conocemos los gobiernos que las están adquiriendo, México como uno de los principales que las adquiere y ya conocemos que se están ejecutando estos programas, estos *software*s y todo este tipo de medidas.

La gravedad no está nada más en que las empresas lo estén desarrollando, sino también en la regulación sin la justificación que mencioné en este momento. O sea, no era nada más la Ley Telecom, justo el 2 de enero de este año entraron en vigor los lineamientos que publicó el Instituto Federal de Telecomunicaciones, los cuales regulan los dos artículos muy controvertidos de la Ley Telecom y ahí se establece con más precisión la obligación de todas estas empresas, que son muy conocidas como intermediarios, pero es que incluyen empresas de telefonía, empresas proveedoras de Internet, etcétera.

Incluso los lineamientos en su momento, desde Artículo 19 también ya solicitamos al INAI que ejerciera una acción de inconstitucionalidad, aunque los lineamientos no podrían ser considerados una norma general para efectos de, ya sea del amparo o de la acción de inconstitucionalidad, ya hay un antecedente donde se cuestionó la proporcionalidad de la portabilidad de unos lineamientos del IFT.

¿Por qué lo menciono? Porque el IFT es un órgano regulador que va determinando todas las prácticas estándares utilizables, aplicables o no, en el uso de las telecomunicaciones y todo ello impacta en los sistemas de vigilancia masiva que se están implementando en México.

¿Por qué? Porque también a nivel internacional y nacional las organizaciones que estamos aquí, y muchas que no están, hemos estado luchando una batalla para que el control judicial se establezca en todo tipo de intervención, no nada más las intervenciones en la telefonía, o sea, tiene que ver con intervenciones también a toda la retención y compilación de los datos que están obligados las empresas a hacer, a donde te muevas, los registros de las llamadas con las que te comuniques, toda tu geolocalización, no requieren un control judicial, únicamente hay una modalidad, que es la de las comunicaciones, que tiene que ver con contenido de la comunicación.

Pero el IFT replicó tal modalidad sin contemplar unos controles judiciales que pudieran garantizar la protección de los datos y la información de los que estamos usando telefonía móvil, todos nuestros datos y toda nuestra información en Internet.

Entonces, lo menciono justo porque se está regulando, no nada más se está aplicando un sistema de vigilancia, sino hay temas muy preocupantes en la regulación, que si bien existe el amparo, una acción de inconstitucionalidad, estamos entrando a una judicialización de un derecho, un derecho en que no tendría por qué recurrirse a tal etapa para poder protegerlo y garantizarlo.

Esto incluso implica procesos que están impactando directamente nuestra privacidad en nuestra protección de datos y, por ende, nuestra libertad de expresión. O sea, desde Artículo 19 tomo un ejemplo que Katitza me dio antes que iniciáramos la reunión, la ponencia, específicamente Robles Maloof nos menciona también la manera en que han sido vigilados defensores y defensoras en sus redes sociales.

Por otro lado, en Twitter tenemos personas que también se dedican a difundir temas de corrupción, temas de ataque, temas de arbitrariedades por parte de las autoridades y existen estos sistemas automatizados, conocidos como *bots,* que terminan aislando la discusión central e importante, que es de interés público y convirtiéndose en una discusión ya no tan relevante para el interés público.

Este tipo de sistemas también están siendo hoy en día, por lo menos Twitter, que hace unos meses vino como a reunirse con varias organizaciones para conocer nuestras mayores preocupaciones, los *bots* fueron una de ellas, pero tampoco pueden garantizar protecciones justo por la libre utilización y la libre opinión que manejan las políticas de Twitter.

Además de eso tenemos casos ya documentados donde estas personas que empiezan a ser hostigadas, incluso ya no son hostigadas nada más por personas, funcionarios públicos que desde sus cuentas de Twitter oficiales, sino también terminan siendo publicadas fotos de ellos en todos los lugares donde los tiren.

O sea, la vigilancia ya no es ubicada nada más en tu ámbito digital, sino que es transferida al físico, donde te pueden ubicar y, como se ha dicho muchas veces, esto determina la seguridad y la protección de la vida de muchas personas.

Todo esto lo menciono por el efecto que tiene en la libertad de expresión una falta de protección a estos derechos de privacidad y datos personales en Internet.

Para pasar a otro tema, quería también mencionar que la corresponsabilidad de la que se ha estado hablando, me parece que tendríamos que tener mucho cuidado con los discursos que utilizamos muchas veces de si renunciamos a la privacidad para tener otros beneficios en los usos de los servicios de Internet, o incluso cuando se llega a decir que ya no existe la privacidad en la red.

Porque aplicar este tipo de discursos como tales y como absolutos, cualquier medida que hiciéramos de autoprotección o de auto cuidado sería innecesaria.

Esta protección, en vista de todos los sistemas de vigilancia que se ejercen en todo el mundo, el Relator Especial para la Promoción y Protección del Derecho a la Libertad de Expresión ya se pronunció al respecto sobre la encriptación y el cifrado de comunicaciones.

Las personas, ante esta vulnerabilidad a sus derechos a la privacidad, encuentran un nicho de protección en estos mecanismos, donde el

anonimato es importante y donde la encriptación es importante. Y de esta manera se protege el derecho a la libertad de expresión por el efecto inhibidor que ha tenido todo el sistema de vigilancia y todo el sistema de retención, tratamiento y regulación de vigilancia en México.

Por eso quería nada más plantear estos dos aspectos que ya se están empezando a discutir a nivel internacional y donde muchos países están no a favor de estos mecanismos de encriptación y anonimato, que dicen que de esta manera utilizar, por ejemplo, los mensajes cifrados, a las autoridades de seguridad pública e inteligencia les limita sus labores de persecución de delitos, procuración de justicia.

Pero, por el otro lado, como ya nos lo mencionó Jesús, toda la inversión que se está haciendo en la vigilancia no está orientada a la investigación y persecución de delitos, se está ejerciendo de otra manera y a otros espacios donde, repito lo que dijo él, se inhibe a la disidencia.

El derecho a la libertad de expresión es tal cual que tú puedas mantener esa opinión por muy crítica que sea y ese mensaje crítico que tengas hacia cualquier personalidad pública, también debe estar protegido en este espacio. O sea, la necesidad de proteger el derecho a la libertad de expresión no es nada más la libertad de expresión. En el ámbito digital es proteger el espacio donde estás ejerciendo tu libertad de expresión.

A mí me gustaría nada más cerrar rápido con este mensaje, donde esta desconfianza que tenemos hoy en día hacia la tecnología únicamente va a ser mitigada en la medida en que nuestra protección esté garantizada también en Internet y así seguir ejerciendo nuestra libertad de expresión de manera libre e independiente.

Muchas gracias.

Mtro. Alejandro Torres Rogelio: Muchas gracias, Paulina.

Además, quizá mencionar que no solamente las autoridades, los políticos y los gobiernos violan derechos, no solamente son la única amenaza a la libertad de expresión y a la privacidad, también particulares, empresas, pero también crimen organizado. Ya hemos

tenido casos de blogueros y por supuesto twitteros que han sido agredidos, amenazados y lamentablemente algunos asesinados precisamente por sus publicaciones y su activismo en redes sociales. Es algo de lo que hay que abordar también.

Nadie se está negando a una cuestión en que haya trabajo de inteligencia, que haya trabajo de investigación en contra del crimen y todo ello, por supuesto que eso es necesario para protegernos, el problema son las reglas, cómo se hace esta vigilancia y estos mecanismos que se están utilizando, tanto *hardware* como *software*, las reglas del juego finalmente y todo lo que implica.

De eso va precisamente este debate.

Yo quisiera agradecerles a todas ustedes, a todos ustedes que participaron hoy, esta tarde, en este panel, para poner estos temas en la mesa, que son temas que se seguirán discutiendo en diferentes foros.

El InfoDF les agradece muchísimo que hayan aceptado esta invitación para estar esta tarde con nosotros. De verdad, muchísimas gracias.

Presentador: A continuación el Comisionado Ciudadano del InfoDF, Alejandro Torres Rogelio, hará entrega de los reconocimientos a los panelistas:

Hace entrega a Carlos Martínez Velázquez. También entrega el reconocimiento a Jesús Robles Maloof. Hace entrega a Paulina Gutiérrez. Entrega el reconocimiento a Jorge Flores Fernández. Y por último, hace entrega del reconocimiento a Katitza Rodríguez.

Brindémosles un fuerte aplauso.

Invitamos a los integrantes del panel a tomarse la foto del evento.

- - -o0o- - -