COPENHAGUE – Discusión intercomunitaria con los comisionados de protección de datos
Lunes, 13 de marzo de 2017 – 15:15 a 16:45 CET
ICANN58 | Copenhague, Dinamarca

NIGEL HICKSON: Vamos a empezar esta sesión en unos minutos pero quisiera pedirles a todos que vengan aquí al frente. No somos contagiosos. Si quieren venir al frente, se lo agradeceremos.

JAMES BLADEL: Buenas tardes. Queremos pedirles a todos por favor que tomen asiento. Como decía Nigel, siéntanse cómodos en venir aquí al frente. Tenemos mucho espacio. Quizá la sala fue un poco optimista para la audiencia que estamos teniendo hoy pero siéntanse cómodos para venir aquí al frente. Vamos a empezar en aproximadamente 100 segundos.

Buenas tardes otra vez. Bienvenidos a esta sesión intercomunitaria. Nuestro tema hoy es el de la privacidad de datos. Está realizado por el Consejo de Protección de Datos y el Comité Gubernamental. Tenemos aquí a expertos del Consejo de Europa y en representación de la comunidad acompáñenme en recibir a estas personas que están recién llegadas a Copenhague.

El tema de la privacidad de datos afecta a todos los actores, ya que sea que representen al gobierno, a los registros o a los

registradores, o incluso si estamos nosotros dentro de los millones de registratarios en Europa y en el mundo. Casi todos los aspectos que protegen la privacidad de datos impactan y desafían el trabajo que hacemos aquí en la ICANN. Esta sesión especialmente vemos que viene en un buen momento porque nosotros en la GNSO estamos trabajando en las cuestiones de política y analizamos los sistemas de registración de datos. Esperamos que esta sesión informe este trabajo. En nuestras discusiones de hoy vamos a dar inicio a la colaboración continua y al diálogo con todas las organizaciones.

Dicho esto, vamos ahora a empezar con lo que yo espero que sea una sesión interesante. Esta vez quisiera darle la bienvenida a Johannes Kleijssen, del Consejo de Europa. Es el director de la sociedad de la información y la acción contra el delito. Tiene algunos comentarios iniciales.

JOHANNES KLEIJSSEN: Muchas gracias, Presidente. Buenas tardes a todos. Estoy muy contento, muy agradecido a la GNSO, al GAC y a la junta directiva de la ICANN por recibirnos aquí y por haber apoyado la propuesta del Consejo de Europa para esta discusión intercomunitaria. Vamos a contarles qué hace el Consejo de Europa y quiénes somos en algunos minutos.

Estamos constituidos por 47 estados y 5 observadores. Estamos en 49 países. Nos ocupamos de derechos humanos y el imperio de la ley. La sociedad civil ha trabajado con nosotros en los últimos 30 años. Tenemos una plataforma para la cooperación con la comunidad comercial y le damos ahora ya un estatus formal. El Consejo de Europa cada vez más está siendo una organización intergubernamental y está pasando cada vez más a ser una organización de múltiples partes interesadas no como el que encontramos aquí en ICANN.

Escuché a varios de ustedes. Algunos de ustedes seguramente me escucharon a mí en Estrasburgo en la Convención sobre Derechos Humanos. Hemos defendido los Derechos Humanos pero queremos también asegurar que haya gente de la aplicación de la ley. Tenemos más de 60 convenciones internacionales que se ocupan de derecho penal. Por eso también queremos trabajar con ambos. Tenemos un observador en el GAC desde el año 2010. Hasta ahora hemos presentado tres informes para discusión, uno de los cuales está siendo debatido esta misma semana.

En la sesión de hoy vemos mucha relevancia a la Convención de Protección de Datos, también llamada Convención 108, que reúne a 50 estados que han ratificado la convención. Tenemos también 10 observadores que han presentado la mitad de los

estados mundiales que tienen legislación de protección de datos. Esto va mucho más allá de Europa, por supuesto.

La contraparte de esta convención seguramente es la Convención sobre el Ciberdelito, también conocida como Convención de Budapest. Hasta ahora el único instrumento internacional en este campo que también tiene 50 estados contratantes, incluidos Estados Unidos y Francia. Estamos trabajando con 125 países en todo el mundo sobre la generación de capacidad.

Para el evento de hoy esperamos que esta discusión sea el principio de un proceso y no un evento que ocurra una sola vez. Estamos convencidos de que se trata de algo que se hace a tiempo. Hay que tener esta discusión en este momento y esperamos que aquellos de ustedes que siguen siendo escépticos puedan estar convencidos al finalizar esta conversación, después de haber escuchado de los comisionados de protección de datos que este es un diálogo necesario porque cada vez hay más obligaciones legales de las partes contratantes entre sus obligaciones y el derecho internacional e ICANN. Esto se aplica entonces también a ICANN en sí. Esperamos que la discusión de hoy sea el comienzo de un proceso que nos lleve a soluciones de múltiples partes interesadas significativas. Muchas gracias.

BECKY BURR: Hola. Todos saben que yo estoy dividida entre la ICANN y la ley privada y la política. A veces en ICANN estas cosas se chocan pero hasta que yo me uní a la junta directiva tuve que ocuparme de cada una de las revisiones del WHOIS, hasta que llegué aquí. Creo que muchos de ustedes han dicho que nosotros necesitamos autoridades de protección de datos para que estén aquí. Yo estoy muy agradecida por el esponsoreo del Consejo de Europa y las sociedades de protección de datos que están conversando con nosotros en este diálogo. Ustedes escucharon que esta no va a ser una conversación de una sola vez sino que tienen la intención de que sea un diálogo abierto, inclusivo y que no se termine.

Voy a presentar ahora a los panelistas. Tengo primero una ronda de preguntas. Luego vamos a pasar a las preguntas del piso y cualquiera que esté participando en forma remota. Primero voy a comenzar con alguien que está en el panel, que no necesita presentación, que es uno de los patrocinadores. Es el señor Thomas Schneider. Es el presidente del GAC y el vicepresidente del Servicio de Asuntos Internacionales y el coordinador de la Sociedad de la Información Internacional en Suiza. Lo tuve que leer porque es una descripción realmente muy larga. Thomas está aquí y va a dar inicio a las preguntas. También tenemos a Giovanni Buttarelli, el supervisor de protección de datos, quien

fue designado en ese puesto por el Parlamento y el Consejo de Europa por un periodo de cinco años en el año 2014. Él trabajo en esa oficina anteriormente y antes de eso fue el secretario general de la autoridad de protección de datos italiana desde 1997, que es prácticamente desde el principio de los tiempos en este mundo de la privacidad de Internet.

Wilbert Tomesen es el vicepresidente de la Comisión de Protección de Datos de los Países Bajos y también el vicepresidente del grupo de trabajo del artículo 29. Me recordó hoy que el artículo 29 primero se contactó con ICANN en el año 2004 y desde ese momento hemos estado manteniendo correspondencia en forma regular. Joe Cannataci es el relator especial de la ONU para las cuestiones de privacidad. Él estudió en la Universidad de Malta y también está en el grupo de tecnología dentro de la facultad de Derecho en la universidad de Groningen. Espero haberlo pronunciado bien. También él enseña. Es profesor adjunto en una universidad en Australia. Todos ustedes, los tecnológicos que están esperando recibir una discusión de política continua pueden ver que él es profesor en una universidad del Reino Unido y también trabaja en la ciudad de computadoras británica.

Tenemos a Caroline Goemans-Dorny, que proviene de la INTERPOL. En esa capacidad, ella monitorea los procesos de cumplimiento y trabaja con 190 funcionarios de protección de

datos que son designados en cada una de las oficinas centrales de la INTERPOL. Luego tenemos a Gail Slater que está en este costado. Gail es vicepresidente de las actividades regulatorias de la sociedad de Internet. Ella tiene una carrera que comenzó muy cerca de mi corazón. Antes de unirse a la Sociedad de Internet en el año 2014 le dedicó más de una década a la Comisión de Comercio de Estados Unidos y trabajó con un asesor. Hay también expertos aquí en el panel que seguramente se van a acordar de Julie, que trabajó con la autoridad de protección de datos. Quiero comentarle también algo a Michele. Gail tiene la doble nacionalidad, estadounidense e irlandesa. Tuvo un título de máster en Derecho Europeo.

Finalmente, Jim Galvin, otra persona que no necesita presentación. Está en el Comité Asesor de Seguridad y Estabilidad de la ICANN desde su primer año y ha sido un participante muy activo en el IETF desde hace más de 20 años. También es el director de relaciones estratégicas y estándares tecnológicos en Afilias. Tenemos entonces aquí un excelente panel. Esperamos también que haya alguna experiencia. Sabemos que hay algunas personas que seguramente van a querer escuchar sobre estos temas. Quiero empezar por hacerles algunas preguntas introductorias. Le voy a dar la palabra primero al señor Buttarelli. Giovanni, ¿podría por favor contarnos brevemente algunos de los principios fundamentales

de la privacidad que son el fundamento de las leyes de protección de datos, incluyendo las regulaciones de protección de datos que van a aparecer pronto?

GIOVANNI BUTTARELLI: Muchas gracias, Becky, por esa presentación. Les quiero dar la bienvenida a todos. Mi rol es el de actuar como alguien que va a romper el hielo. Voy a empezar por decirles que los principios que quiero mencionar brevemente no son solamente principios de la Unión Europea o están contenidos en la convención del Consejo de Europa, la 108, porque cada vez más la protección de datos se convierte en algo global. Hemos empezado a identificar 120 países en el mundo que ahora están equipados con las leyes de moderna generación sobre la privacidad de los datos. Ellos se están alejando de un sistema de autorregulación y a pesar de que algunos principios se mencionan en forma diferente, como por ejemplo el principio de limitación de propósito, hay muchas similitudes y hay muchas que están trabajando en el mundo de un modo que cada vez crece más.

Quisiera ahora también pedirles que no piensen que la protección de datos es simplemente una carga administrativa y algo aburrido en lo que se refiere a la gobernanza de Internet. En una perspectiva general se puede ver que en junio de 2014 se publicó en el sitio web de mi institución lo que puede ser el rol

europeo en el futuro de la gobernanza de Internet en términos de los valores democráticos, en términos de las relaciones con las múltiples partes interesadas para la estructura de la gobernanza y también con relación a la necesidad para promover una red única y no fragmentada en todo el mundo.

La privacidad se considera en todo el mundo como un derecho fundamental, como un derecho esencial, mientras que la protección de datos comenzó a ser considerada como tal en Europa y en algunos otros países pero esencialmente la protección es tanto de los datos como de la privacidad. Eso se considera por muchas leyes en el mundo como un prerrequisito para beneficiar a otros derechos fundamentales, incluyendo la libertad de expresión, el derecho a la identidad personal y, más recientemente, a la dignidad. Por eso mi institución el año próximo va a acoger la Comisión Internacional sobre la Privacidad y la Protección de datos para focalizarse en la ética y en la nueva tecnología. Tenemos también las cuestiones de la transparencia, que se refieren a la claridad sobre quién está haciendo qué cosa. Por eso, las nuevas definiciones adoptadas no solamente pero en Europa sobre el rol de un controlador, de una persona que se encargue de procesos, son claves para identificar un marco adecuado en términos de la rendición de cuentas.

La legalidad y la justicia son cosas que se deben mencionar también. La legalidad no solamente quiere decir tener un fundamento legal para procesar los datos. Tiene que haber una relación contractual, un interés legítimo, una relación de contribución, un interés vital del controlador de una tercera parte pero también tiene que haber consistencia y cumplimiento con todas las otras legislaciones correspondientes, incluyendo aquellas que no se vinculan con la protección de datos como los derechos de autor, como también el derecho que protege al consumidor. La privacidad por diseño y la privacidad por defecto ahora están incluidas en los nuevos principios de Europa y deben ser respetados. El reciente marco regional en la Unión Europea apunta a reforzar las facultades de supervisión de las autoridades competentes y pretende modernizar los marcos de protección de datos al tener un enfoque más coherente para que los controladores no fragmenten sus políticas dependiendo de los territorios. Queremos también tener unos controladores más responsables. Es decir, que las autoridades de protección de datos sean más selectivas. Quiere decir también que los controladores tienen que hacer un poco más la tarea en la identificación de una política sustentable y también en identificar los riesgos específicos, asignar responsabilidades, demostrar que uno cumple con la política más adecuada.

Este marco legal solía aplicarse a los individuos. Es decir, a las personas, pero no a todas las personas. Los grandes datos son clave aquí. Allí hay que identificar también el impacto de este marco legal en todos los datos personales que se vinculan con los individuos que actúan en representación de una empresa, por ejemplo, o una administración pública. Voy a hablar en una segunda ronda sobre las limitaciones pero quiere decir que 13 años después del evento de ICANN en Roma, nosotros quisiéramos poder volver a la pregunta que planteamos en el año 2003 donde empezamos a hacer tres preguntas a la comunidad. Primero, la pregunta era: ¿Por qué un registro de nombres de dominio en Internet tiene que ser tratado de modo diferente a un directorio de telecomunicaciones cuando se registra un nombre de dominio? Es decir, el derecho a no ser incluido en un registro.

Una segunda pregunta es cómo este principio se traduce en la práctica. La pregunta es: ¿Existe algún otro método menos intrusivo comparado con la publicación obligatoria que tenga el mismo objetivo que el WHOIS sin que todos los datos estén disponibles online directamente a todo el mundo? La otra pregunta se vincula con el acceso en masa al marketing directo. También queremos tratar de darles una sugerencia en lo que se refiere al acceso por terceros. Nuestra suposición es que hace 13 años, y la conclusión para mí sigue siendo válida, y cito en un

segundo la oración específica, el objetivo del directorio de WHOIS no puede extenderse a otros objetivos simplemente porque son considerados deseables por algunos usuarios potenciales de esos directorios.

Este es un ejemplo que puede ayudar en la identificación de cuáles son estos objetivos, estos propósitos. Nosotros quisiéramos que estos principios sean efectivos en la práctica. Aquí no se trata de un problema de la Unión Europea versus Estados Unidos. Esto tiene una dimensión global y va a servir para reforzar la confianza en Internet. Nosotros somos lo suficientemente flexibles como para hacer que este principio sea efectivo en la práctica y vamos a requerir unas protecciones, unas salvaguardas porque al final estamos todos del mismo lado.

BECKY BURR: Muchísimas gracias. Quisiera pedirle que hable un poco más, Wilbert, sobre las limitaciones y los principios en relación a la responsabilidad que son importantes para nuestros debates.

WILBERT TOMESEN: Seguramente voy a superponer algunos puntos con Giovanni pero quiero hacer una especie de confesión porque yo he sido durante muchos años, unos 25 años, estuve en las leyes y

también fui supervisor. La combinación de estas tareas le hace pensar a uno que uno ha visto todo, que sabe todo, pero esto no es así. Muchas veces estoy sorprendido por el tamaño y por la atmósfera de esta reunión. Quiero agradecerles por haberme invitado a participar porque es un evento muy importante. Durante muchos años, Giovanni ya lo ha dicho, uno ha seguido muy de cerca muchos debates en relación a la ICANN, por ejemplo. Hablamos de la disponibilidad pública de los datos del WHOIS. Yo he participado de esos temas. También las implicancias que tiene esta cuestión del WHOIS. Esto nos hace reunirnos en forma presencial y confrontar en algunos debates después de nuestras presentaciones.

Los europeos, damas y caballeros, tienen la expectativa, por ley, de que sus datos personales solamente van a ser procesados con un propósito legítimo y que no van a ser utilizados con ninguna otra finalidad. Esto significa que todos los datos personales van a ser tratados en un proceso que sea justo, legal y transparente. Estos son los principios básicos establecidos ya en nuestra directiva y también, por supuesto, en la ley europea, lo cual significa que básicamente nosotros deberíamos controlar y también recabar de los controladores datos o información para propósitos específicos, con procesos y maneras que sean compatibles con los procesos establecidos, con los principios

establecidos, lo que nosotros denominamos la limitación del propósito.

En segundo lugar tenemos un principio general o abarcativo que es que los datos que uno procesa deben ser adecuados y relevantes para el propósito para el que son necesarios. Esto es lo que nosotros denominamos la minimización de los datos. El proceso tiene que ser de alguna manera predecible, justo y transparente, como acaba de decir mi colega, en un contexto en el cual siempre tratamos de disminuir la minimización. Uno puede, por ejemplo, leer en algunos documentos como en los de Tim Berners-Lee, que dicen que a veces estamos perdiendo el control de los datos personales. Hasta donde yo entiendo, estamos ocupados de la supervisión de estos datos y de ser también justos, transparentes y predecibles en el trabajo y la administración de los datos de acuerdo con lo que establece la ley. Estos son principios generales y no son negociables.

Quiero señalar esto pero también quiero decir, con respecto a la disponibilidad pública de los datos de WHOIS, que pensemos en los principios, por ejemplo, en la limitación de los propósitos. Ustedes saben mejor que yo que el propósito del WHOIS es poner a disposición los datos de contacto del WHOIS. El propósito del WHOIS ha sido expandido para acceso público a las agencias de cumplimiento de la ley, a los titulares de derecho, a los que hacen solicitudes en materia de seguridad. Damas y caballeros,

estos utilizan datos para usos legítimos porque, como dijimos anteriormente, es un propósito útil. Para que ICANN, para que ustedes puedan tener estos datos personales publicados, es necesario que exista un proceso de publicaciones que proteja la privacidad y los intereses de privacidad de los usuarios.

También recibimos diferentes reclamos de personas sobre la disponibilidad pública de los datos personales y de los datos de contacto que se expresan a través del WHOIS. Estos datos se publican en muchos sitios web y están también disponibles prácticamente para todo el mundo, para cualquier propósito, ya sea bueno o sea malo. Este sería mi primer comentario. Quisiera expresarme y expandirme un poco más en mi comentario porque es esto lo que quiero contarles.

El objetivo principal de las nuevas regulaciones, como dije anteriormente, es tener un proceso transparente, justo y predecible para tratar datos personales en todas partes del mundo. Esto significa que, para ser responsables ante ustedes, nosotros tenemos que poder cumplir o demostrar nuestro cumplimiento con los DPA a través de los requisitos legales. Otra vez, aquí hay una necesidad de hacer un procesamiento de datos y tener en cuenta la limitación de estos datos. Sin lugar a dudas, también vamos a ser evaluados por cada país y por cada DPA en la Unión Europea. Los DPA, por supuesto, han estado ejerciendo su poder también en este sentido. Al mismo tiempo, voy a decir

que estoy convencido de que hay organizaciones que toman en cuenta estas reglas con principios fundamentales y tratan de implementar estas reglas de principios fundamentales y también ganar la confianza y el respeto de sus consumidores.

BECKY BURR: Gracias, Wilbert. Le voy a dar la palabra ahora al profesor Cannataci. Joe, por favor, ¿podría hablar del acceso de terceros a los datos? Esta es una cuestión bastante importante para esta organización en el contexto dentro del WHOIS y también en el contexto de algunas cuestiones de la custodia de datos. ¿Podría, por favor, hablar entonces del acceso a los datos de terceros?

JOSEPH CANNATACI: Gracias, Becky. Quiero, en primer lugar, agradecerles a los organizadores por poner a disposición este tema. Yo creo que primero sería mejor comenzar hablando de algunas cuestiones que han mencionado Giovanni Buttarelli y también otros colegas. Cuando nosotros hablamos del acceso por parte de terceros tenemos que tener en cuenta la forma en la cual las leyes de privacidad y protección de datos se aplican y cómo surgen. En realidad surgieron en los Estados Unidos alrededor de 1967 y 1973. También tuvieron lugar en Europa posteriormente.

Fueron creadas de la siguiente manera. Si uno va a brindar datos para un determinado propósito, uno supone que va a dar esos datos para ese propósito únicamente o para un propósito que es muy compatible con ese propósito inicial. Si alguien recaba mis datos dentro de un contexto bancario para obtener un préstamo, por ejemplo, uno va a utilizar esos datos para ese propósito en particular. Puede también tener una política de seguros pero no va a haber otro propósito más allá de eso, etc.

Cuando nosotros hablamos del acceso por parte de terceros creo que tenemos que tener en cuenta que este es un contexto en el cual lo tenemos que debatir. en segundo lugar, creo que podemos ver la forma en la cual las cosas han cambiado de modo tal que si yo por ejemplo vuelvo o me retrotraigo unos 33 años, cuando comenzamos con todo estos debates, para proteger los datos de la policía, y aquí tienen a Caroline, quien también tiene que ver con la protección de datos. Está involucrada en la protección de datos. Se aplica el mismo principio. Uno también tiene que tomar en cuenta cuidadosamente las primeras recomendaciones y regulaciones que emitió el Consejo de Europa. Todas ellas estaban construidas sobre la base de que los controladores de datos iban a realizar la mayor parte de la recabación de estos datos y que las fuerzas policiales iban a recabar todos esos datos para sí. Por

ejemplo, los proveedores de servicios de salud también iban a recabar esa información.

Hoy en día tenemos una realidad y es que hay una distancia considerable que existe entre la policía o un proveedor de servicios de salud o un proveedor farmacéutico, no necesariamente porque recaban los datos en sí mismos sino también porque dependen de los datos que otras personas recaban. A veces también hay datos que son recabados muy a menudo por compañías privadas y muchas veces los ciudadanos no están al tanto de todo esto. Esto es particularmente importante en una serie de contextos, porque si uno tiene que preguntarles a una serie de compañías que operan en Internet, les van a decir que ellos enfrentan cientos de miles de solicitudes de acceso tanto a metadatos como a datos de contenido. Esto no solamente se da en un contexto de cumplimiento de la ley o en un contexto de inteligencia, aunque son contextos muy importantes. Muchas veces hay una sola compañía que puede enfrentar o recibir 17.000 solicitudes y por lo tanto tiene mucha presión, no solamente a nivel de la compañía sino también en relación a los sistemas legales. No tenemos tiempo de abordar todo esto.

Si hubiera un fiscal, por ejemplo, uno podría encarar un procedimiento legal. Podría dar lugar, por ejemplo, a un procedimiento de 11 a 13 meses para poder acceder a los datos.

El acceso de terceros es cada vez más complejo. Es una situación, un tema cada vez más complejo. Cada vez es más complejo por el hecho de que hay una serie de gobiernos, lo que incluye a los gobiernos europeos, los Estados Unidos y al gobierno australiano y de Nueva Zelanda, una gran cantidad de gobiernos que han declarado que algo es tan sagrado en realidad como podríamos decir la mismísima Virgen que es el principio de datos abiertos.

Hace 30 años, esto no era así y ahora teníamos que pensar en una medida de protección. Seguimos avanzando. Cuando hay grandes datos y hay análisis para poder triangular estos datos, llegamos a datos abiertos y muchos llegan a un punto y dicen: "Caramba, este propósito de los datos que básicamente es lo que uno hace, este triple propósito de tener datos grandes, datos abiertos, implica que uno le está dando a terceros acceso que se transforma en un tema de tener que cambiar la política pública". Estas son muchas de las cuestiones que son de relevancia y de importancia para los terceros y que son también muy importante dentro del ambiente de la ICANN, porque dentro del ambiente de la ICANN, la ICANN ayuda a brindar una mejor infraestructura tecnológica. Ayuda a que la gente se conecte entre sí y debe también brindar una manera de implementar ciertas decisiones en materia de política. En este sentido, hay que tener en cuenta esto.

En lo que se refiere al acceso de terceros, también tenemos que recordar el contexto de la infraestructura legal y de las políticas que todos los estados implementan y a las cuales se refería el colega Giovanni Buttarelli. Tenemos entre 100 y 120 estados que han seguido el modelo europeo. Cuando dan acceso a terceros, este acceso a terceros solo puede ser otorgado como regla si, por ejemplo, es para un propósito específico, si es para proteger la seguridad pública, para proteger los intereses monetarios o para evitar diferentes delitos.

Esto se efectúa dentro de un contexto donde existe una ley. Esta ley da un contexto y esta ley da también medidas de protecciones adecuadas. Independientemente de los debates que vayan a surgir en todo este proceso que espero que la ICANN pueda tener con las personas que están presentes, esto también va a seguir avanzando de modo tal que tenemos que ver qué es lo que la gente espera y qué soluciones también esperan. Las empresas esperan poder seguir llevando a cabo sus actividades comerciales en todo el mundo. Los ciudadanos esperan que se protejan sus datos privados y que haya medidas de protección con respecto a los datos personales en todo el mundo.

SI uno va a operar en una Internet que no tenga límites, también espera que haya ciertas protecciones sin fronteras y también medidas en torno a todas estas fronteras. Esperamos que la ICANN pueda también contribuir a identificar cuáles van a ser

estas soluciones, cuáles van a ser estas medidas de protección técnica y también en materia de política. Gracias.

BECKY BURR: Gracias. Me parece que aquí estamos comenzando a pensar en el cumplimiento de la ley por un lado en este debate y también en la protección de datos o en los defensores de la privacidad por otro lado. Este debate es un debate que no termina. Wilbert, por ejemplo, está al tanto y está trabajando. Él fue fiscal y también está dentro de la parte de las universidades. Caroline también es funcionaria de protección de datos en INTERPOL y son quienes nos van a contar sobre estas cuestiones.

CAROLINE GOEMANS-DORNY: Muchas gracias por invitarme a este panel tan interesante. Como ustedes puede que sepan, la INTERPOL es una organización internacional de policía que abarca 190 países miembros y que en realidad actúa en relación a cuestiones de información internacional a nivel mundial para las bases de datos de la policía. Quizá INTERPOL no existiría si tuviese que dedicar esfuerzos e invertir en principios de privacidad de datos desde 1982. Esto nos retrotrae a las bases. ¿Por qué todos estos principios tienen que existir? Para hacer una corporación policial efectiva necesitamos confianza. Necesitamos tener una buena reputación y necesitamos también acortar las brechas,

especialmente porque trabajamos en un ambiente global. Por lo tanto, hay principios de políticas muy sólidos que implementan estándares de protección de datos que hay que tener en cuenta y que nos ayudan.

Nosotros hemos esperado en la INTERPOL que podamos tener una corporación efectiva desde una perspectiva técnica y en realidad implica tomar tiempo para poder crear los fundamentos sólidos de algo que va a ser más sólido. Esto en realidad es una inversión a largo plazo en relación a la protección de los datos. Esto ha estado ocurriendo desde hace varios años. Nosotros hemos estado abordando el tema de las reglas de INTERPOL sobre protección de datos desde 1982. También después de la Convención 108 del Consejo de Europa. Estos principios de privacidad se han continuado desarrollando y se han desarrollado en una especie de código detallado donde hay unas 136 disposiciones. Ha tenido 11 actualizaciones desde 1982. Aproximadamente tenemos una actualización de los estándares en materia de datos cada tres años. Esto implica que hay un proceso que es muy dinámico y realmente flexible, que ayuda a que estos estándares sigan siendo flexibles. Tenemos entonces reglas que son flexibles que se adaptan a los diferentes propósitos.

Por supuesto, este es un desafío continuo. Nuestra última actualización de nuestras reglas se llevó a cabo en noviembre de

2016. Las reglas del organismo de supervisión se reforzaron y ahora estamos trabajando también en una próxima actualización en particular sobre la corporación. Estamos trabajando con el sector privado. Por supuesto, ha habido una gran evolución y este marco tiene que servir para ayudarnos.

Ahora voy a referirme al segundo punto que tiene que ver con el marco de interpretación. Como mencioné anteriormente, esto tiene que ver con los derechos de privacidad y aquí todos los derechos fundamentales están involucrados, también el derecho de libre expresión. La constitución de la INTERPOL se refiere expresamente a la declaración de derechos humanos y también señala los principios organizacionales de neutralidad que en realidad significa que la organización no puede interferir en cuestiones políticas, religiosas o militares o raciales. Estas reglas fundamentales también se ven reflejadas en la actualización de todos estos procedimientos y políticas. Quizá este es el valor de INTERPOL. INTERPOL puede actuar como un centro de información. Hay un equipo multidisciplinario de policía, de funcionarios, que trabajan día y noche en diferentes turnos para poder revisar más de 3.000 solicitudes mensuales que se reciben de diferentes países que buscan información o que piden la ubicación o el arresto de determinadas personas.

Estas solicitudes se revisan teniendo en cuenta la legalidad y la calidad. También se utilizan ciertas herramientas de calidad y

automatizadas como por ejemplo la ubicación de ciertas palabras. Además se observa el cumplimiento de ciertos criterios específicos. Este rol de centro de información es muy importante porque hace que la corporación sea más efectiva. Finalmente, creo que la fortaleza de los principios globales subyace en la posibilidad de hacer difusión a nivel global y de poder acortar las brechas que existen en los diferentes procesos legales, en las diferentes leyes. Esto va a crear una cierta interoperabilidad para pode realizar las cosas, no solamente en materia técnica. Estos estándares se basan en diferentes pilares. Tienen que ver con la implementación. También hay pilares para otros estándares. Se basan en la efectividad de la implementación, en la extensión de las capacidades, en una buena supervisión y también en los recursos para los individuos. Estos estándares de INTERPOL han sido adoptados por los 190 países que son miembros. INTERPOL es una corporación voluntaria. Se compone de miembros que desean contribuir. Las medidas son vinculantes y se pueden imponer sanciones.

Finalmente, hay principios que derivan en principios de protección de datos y que también afectan a los principios gubernamentales. ¿Cuál es el propósito? ¿Para qué se tiene un proceso? Para la legitimidad. ¿Cómo se lleva a cabo? Transparencia. Para legitimar el cumplimiento. Estos son todos los principios gubernamentales que también llevan a una buena

actividad. Voy a terminar diciendo que creo que no tenemos que ocuparnos únicamente de los estándares legales o implementar principios de privacidad. Este es un proceso continuo, holístico. Tiene que ver con las regulaciones, con los procesos comerciales, con los diferentes derechos a la tecnología y, por supuesto, es algo muy desafiante. No tenemos que olvidarnos de que es un aspecto muy importante, un componente muy importante que ya ha sido planteado y que también tiene que ver con la ética. Esto establece lo que se puede hacer, lo que no se puede hacer y lo que se debería o no se debería hacer. Esto es muy importante tenerlo en cuenta en Internet.

BECKY BURR: Gracias, Caroline. Thomas ha sido un participante en el GAC en esta discusión y diálogo sin fin. Quisiera tener su perspectiva sobre el pensamiento del GAC a medida que entramos en esta fase renovada del diálogo.

THOMAS SCHNEIDER: Buenos días y bienvenidos a todos. Quisiera agradecer al Consejo de Europa primero por esta iniciativa que nosotros apoyamos fuertemente. Consideramos que es muy relevante tener esta conversación aquí y ahora en Copenhague porque cada vez más somos conscientes, al igual que todo el resto del mundo, que la privacidad, la protección de datos y la política de

los datos que va mucho más allá de la cuestión de la privacidad es una de las cuestiones clave para los negocios, para las instituciones, para los gobiernos que tienen funciones como ICANN que no necesariamente están focalizados en la privacidad. Cada vez nos enfrentamos más a los datos cuando todo el mundo lo está haciendo.

La clave entonces es que el uso de datos cada vez es mayor. El recurso núcleo para la innovación económica. Está siendo una herramienta que nos permite que nuestras vidas sean más cómodas, más seguras y tiene un enorme potencial para la innovación. Al mismo tiempo, hay enormes riesgos de abuso, de utilización incorrecta de los datos, de la pérdida de control. La gente está sintiendo que pierde el control de sus datos. Hay desafíos centrales para todos nosotros. Uno de esos desafíos no es solo para nosotros sino también para los ciudadanos en general y especialmente para las empresas. Tenemos distintas jurisdicciones con distintas normas, distinta legislación pero también dentro del país hay distintas partes del gobierno que tienen distintas funciones. Algunas se supone que tienen que proteger los derechos humanos de los ciudadanos y otras tienen que perseguir a los criminales. Muchas veces las empresas están en el medio entre estos dos socios. Hay una administración a nivel nacional y otras a niveles más globales.

Muchas veces terminamos con expectativas que entran en conflicto de las empresas y los gobiernos pero también de parte de los consumidores que exigen servicios. Al mismo tiempo, exigen que se protejan sus datos y quieren también que sus datos se puedan esparcir por todo el mundo. Para quienes ofrecen estos servicios, este es un desafío específico porque no saben qué hacer. Cuando Johannes Kleijssen dijo antes que el Consejo de Europa también se está convirtiendo en una institución de múltiples partes interesadas, esto es algo que yo puedo confirmar después de más de 10 años de representar a mi país en el Consejo de Europa.

Cada vez más, se está incluyendo a las empresas, a la sociedad civil, a otros expertos y un ejemplo del que yo fui parte en la elaboración como presidente de ese grupo fue por ejemplo cuando el Consejo de Europa estaba estableciendo unas directrices para los ISP. La incorporación de los ISP. Por supuesto, la cooperación con la sociedad civil y los derechos humanos. Mientras estábamos haciendo eso nos dimos cuenta de que la misma institución, y esto también está vinculado a lo que dijo Johannes, la sección sobre el ciberdelito tenía lineamientos para aplicación de la ley para los ISP y nos tomó un tiempo darnos cuenta de que esto estaba sucediendo. Una vez que nos dimos cuenta, hablamos con ellos y tratamos de asegurarnos de que estas directrices para la industria de los ISP

en Europa no entre en conflicto con otras y ellos efectivamente tuvieron que eliminar algunos de estos conflictos antes de que pudiésemos emitirlo.

Allí vemos, entonces, que la gente tiene que salir de sus compartimentos estancos y ver que los comisionados de la protección de datos se comunican con la industria de los dominios de Internet, ver que haya un mayor contacto establecido y por eso agradecemos mucho que este diálogo ahora se extienda a la industria de los nombres de dominio en todo el mundo. También que ICANN pueda aprender un poco más acerca de cómo las regulaciones sobre la privacidad se van desarrollando en distintas regiones del mundo y que aquellos que están en la ICANN generen un marco para los nuevos gTLD o los servicios donde esto se considere un problema, que se puedan desarrollar en la medida de lo posible y en línea con las regulaciones existentes y comunes, para que tanto las empresas como los usuarios finales no estén obligados a decidir entre cuáles son las normas que ellos quieren infringir, si se trata de las de ICANN o de alguna otra. Esto es lo que sucedió en los últimos años.

Voy ahora a hacer un comentario personal. en mi país, donde también tenemos una discusión sobre la política de datos y cuál es el futuro hacia delante, cada vez más gente llega a la conclusión de que la noción de la protección de datos en

términos de prohibir el uso de datos podría no ser la forma más hacia el futuro de implementar los derechos que tenemos en cuanto a la privacidad porque hay beneficios, hay razones por las cuales los datos se deben usar para poder resolver los problemas, para hacer que nuestras vidas sean más fáciles e incluso hasta más cómodas. La cuestión en realidad es pasar hacia unos datos menos prohibitivos y que haya más autodeterminación, que los usuarios puedan decidir quién puede usar esos datos, con qué objetivo y que podamos pensar cómo beneficiarnos de ese potencial que dicta la Internet de las cosas, etc.

Queremos pensar en esta línea para generar una política de datos que se pueda utilizar en el siglo XXI. Esta discusión entonces es parte de la discusión precisamente y esperamos que haya un diálogo interactivo para hablar más concretamente. Por eso decimos que es bueno que esto suceda aquí. Va a continuar en otras cuestiones, en el IGF, el foro de gobernanza de Internet, el cual estamos contentos de poder recibir el 21 de diciembre de este año en Ginebra.

BECKY BURR: Gracias Thomas. Vamos a pasar rápidamente a las preguntas interactivas. Queremos establecer las bases de cómo va a funcionar esto. Gail, las empresas están afectadas por el cambio

en el contenido de los datos del WHOIS. Nosotros trabajamos para estar seguros de que haya un cumplimiento, que todos estemos cumpliendo. ¿Qué es lo que necesita a partir de este diálogo en el cual nos estamos embarcando?

ABIGAIL SLATER: Gracias. Mi nombre es Gail Slater. Vengo de la Asociación de Internet. Estamos basados en Washington D.C. y representamos a más de 40 empresas de Internet. Después de la transición de la IANA, de la cual nosotros no fuimos parte, estamos de todos modos muy orgullosos de decir que pertenecemos a más de 40 organizaciones, incluida la sociedad civil. Estamos apoyando a la NTIA. De hecho, queremos que la comunidad global de Internet participe allí.

Quiero mencionar tres puntos. Creo que tengo unos tres minutos. Lo importante es escuchar sus perspectivas. Desde el punto de vista comercial, creo que es muy importante dar un paso atrás antes de ver cuáles son las necesidades de las empresas, que es la certeza legal, y hablar del contexto más específico de la ICANN. Nosotros estamos en ICANN y la misión y los fundamentos de la ICANN son mantener la estabilidad, confiabilidad, seguridad e interoperabilidad global del DNS. Creo que es un buen argumento decir que la base de datos del WHOIS es clave en ese sentido. Por eso cuando hablamos de los

principios de privacidad, me parece que es muy importante que lo mencionemos en un contexto del WHOIS. Es decir, en un contexto en el que la administración de Obama estaba conforme con las equidades que compiten. Estas equidades que compiten, en lo que se refiere al WHOIS y a las cuestiones de marcas, son bastante equitativas.

También tenemos otras disposiciones para prevenir el spam. Hay algunos que están alineados con la privacidad y otros que están en unos lugares diferentes pero todos compiten entre sí. Es muy importante recordar eso. También quiero mencionar mi investigación en la comunidad de la ICANN y lo que hice en el SSAC en el 2012, algo que recibió un muy buen título: “WHOIS: Un hombre ciego y un elefante”. Se refiere a una parábola india donde hay varios hombres ciegos. Todos tienen que ir a comparar el elefante y todos tocan alguna parte del cuerpo del elefante y cuando vuelven la comparan y están en violento desacuerdo en cuanto a qué es y que no es elefante y cómo se ve. Creo que esta es una muy buen analogía al hablar de estas equidades en el WHOIS.

También hay que reconocer el derecho europeo sobre la privacidad. Si bien la privacidad es un principio muy importante en el sistema de la Unión Europea, tenemos en el sistema de cortes de la Unión Europea un reconocimiento de que tiene que haber un equilibrio entre la observación de los derechos

fundamentales y, por otro lado, el interés del movimiento libre de personas y de datos, el cual es importante en estos momentos. Es importante también que para las empresas se pueda mantener este equilibrio.

También hay una nueva ley europea que va a entrar en vigencia de aquí a 18 meses y va a reconocer este principio en el artículo 6. El punto tres es el que más responde a la pregunta de Becky. Las empresas necesitan certeza legal en este contexto y ahora debemos decir que hay un sistema donde hay equidades que compiten y los principios no están establecidos pero las empresas necesitan esa certeza legal. Si vamos a ver el régimen de privacidad, la primera pregunta es si este régimen es el correcto, si tenemos que tener una discusión sobre cuáles son las mejores políticas para la ICANN en este contexto pero quisiera también destacar que no queda claro y no ha sido planteado hoy si es que esto se aplica a la totalidad de la base de datos del WHOIS o al RDS que puede ser aprobado pronto.

Más del 40% de las entradas en la base de datos del WHOIS están registradas por personas jurídicas y no por personas naturales. El régimen de la Unión Europea solamente se aplica a los individuos. Por eso es importante saber si es que esto se aplica o no en el contexto de la ICANN. Otra pregunta del umbral sería cuáles son los tipos de datos que están implicados en una norma de privacidad que es parecida a la del régimen de la Unión

Europea en el contexto del WHOIS. En el sistema de la UE tenemos una norma que se aplica a lo que se denomina información identificable personal y que puede estar vinculada una persona. Cuando uno mira la base de datos del WHOIS, gran parte de eso es información técnica, no información personal, no información sensible personal. de nuevo, sería muy bueno que las empresas puedan comprender qué es exactamente lo que está incluido en una norma de privacidad en el contexto de WHOIS en lo que se refiere a la información que está allí, qué información se debe establecer. Estas son todas importantes preguntas. La GNSO, la comunidad, espera poder continuar con este diálogo.

BECKY BURR: Gracias, Gail. Por último, el Doctor Galvin. La industria de los nombres de dominio va a estar muy afectada por los estándares. ¿Cuáles son las cuestiones técnicas que debemos tener en cuenta cuando mantenemos esta conversación?

JIM GALVIN: Muchas gracias. Cuando pienso en el diseño y qué es lo que va a requerir que esta comunidad pueda implementar las soluciones que tenemos disponibles para poder cumplir con las necesidades de la privacidad por diseño, a mí me preocupan dos cosas. Primero, la gestión de datos. cada uno de nosotros en la

industria tenemos nuestro propio proceso interno para recolectar datos de un lugar, copiar esos datos a otro lado, almacenarlos, volver a copiarlos para hacer copias de respaldo, luego tenerlos en otra ubicación y a veces hay servicios que quedan en stand by. Tenemos que encontrar otra ubicación para poder brindar servicios adicionales como los reportes, los informes, los servicios como el WHOIS o el próximo RDAP.

La privacidad va a aplicarse a los aspectos a los que vamos a tener que cambiar. Tenemos que pensar en la carga de mover estos datos y posiblemente tengamos que cambiar nuestra propia arquitectura, nuestros procesos internos para poder cumplir con esas necesidades. Algunas de esas soluciones serán más costoefectivas que otras. Vamos a tener un efecto dramático en lo que podemos y no podemos hacer y lo que quizá podamos lograr. Cuando pensamos en las políticas que vamos a ir generando para poder cumplir con estos requisitos de privacidad que nos llegarán, tenemos que pensar en el backend que vamos a tener que tener para enfrentar estos datos que vamos a tener almacenados en distintos lugares. Por eso la gestión de datos es central.

La segunda inquietud que tengo es el acceso a los datos. En el sistema actual tenemos un sistema bastante abierto donde prácticamente todo el mundo accede a todos los datos todo el tiempo. Ese es el sistema que tenemos en el WHOIS en los

servicios de directorio. El otro extremo sería que nadie tenga acceso a ningún dato en ningún momento. Creo que todos vemos que avanzamos hacia un acceso diferenciado. Vamos a tener que tener políticas que encuentren reglas donde se decida quién puede tener acceso a qué y cómo lo va a hacer. Esencialmente vamos a crear un sistema de gestión de credenciales a partir del cual vamos a tener que crear un conjunto de personas, darles ciertas credenciales y luego va a haber algunos de nosotros que vamos a tener que usarlas de un modo para poder validar que se permite el acceso a un conjunto de datos.

Los sistemas de gestión de credenciales varían mucho en su costo desde los poco caros a los muy caros. Hay todo tipo de modos de fallas que pueden ocurrir en este tipo de sistemas y, de hecho, hay unas cargas mucho más grandes asociadas con la mitigación de estas cargas a medida que se van sucediendo. Considerar este tipo de cuestiones implica pensar en cuáles son los sistemas de credenciales que tenemos hoy en nuestra comunidad. Hoy operamos la infraestructura del DNS que es bastante grande y tenemos un sistema bastante grande. Muchos de nosotros tenemos ese sistema que da acceso en tiempo real a los datos. Es decir, que está utilizado el 100% del tiempo. En un sistema de credenciales tenemos que tener un sistema de

validación y tenemos que saber que si les dieron credenciales, las puedo conseguir.

La presunción es que tiene que haber algún tipo de sistema que funcione el 100% del tiempo y que me permita validar esa credencial y saber que está allí. Eso es algo para pensar porque ese es el camino en el que nos vamos a mover. Si no, ¿quién va a ser responsable por esos modos de fallas? ¿Cuál es nuestra posición como comunidad? ¿Cuáles son los tipos de políticas que tenemos que tener para enfrentar estos modos de fallas? Les puedo ofrecer también otra tecnología para pensar. Piensen, por ejemplo, en las certificaciones de autoridad que existen en el mundo. Son infraestructuras donde nosotros hemos visto unas grandes fallas, realmente espectaculares. Tenemos que pensar en nuestras políticas y qué significa para nosotros cuando tenemos este tipo de fallas, cómo vamos a enfrentar estos problemas. ¿Queremos nosotros mitigar estas fallas o acaso las vamos a aceptar cuando sucedan? ¿Cómo vamos a aplicarnos a nosotros mismos reglas que nos permiten aceptarlas y enfrentar que no podemos verlas directamente?

Hay cuestiones de tecnología. Una, por ejemplo, es la gestión de datos. La otra es el acceso a los datos. Tenemos que pensar cuáles son las soluciones que estamos buscando porque el tipo de desempeño y disponibilidad que queramos dar va a impactar

en las necesidades y en cómo las vamos a lograr. Muchas gracias.

BECKY BURR: Vamos a pasar ahora a las preguntas de la audiencia. Aquí ven que hay un micrófono que está justo en el medio, si es que alguien quiere hacer alguna pregunta. Pueden acercarse hasta aquí. Esto va un poco más allá de cuál es el enfoque que uno adopte. Escuchamos que el procedimiento de los datos personales tiene que ser legítimo para poder cumplir con los estándares de transparencia. Hay que poder expresar ese propósito legítimo y el uso tiene que ser proporcional a ese objetivo. No puede ser más pesado que los derechos de privacidad individual. Vamos a tratar entonces de responder a algunas de estas preguntas. Joe, creo que querías hacer un comentario.

JOSEPH CANNATACI: Simplemente quería hacer un breve comentario a lo que se dijo anteriormente. Gail se refería constantemente a la UE, la UE, la UE. Creo que también tendríamos que recordar que el principal tratado en relación a la protección de datos proviene del Consejo de Europa. Esta convención, la Convención 108, es una convención abierta para la firma de los países en todo el mundo. Uruguay la ha firmado. También la han firmado otros países. Hay

varios observadores que la siguen. Lo digo porque, para ser más correctos, yo no quiero ser tan pedante y referirnos únicamente al estándar europeo o hablar únicamente de los europeos. Los estándares de la Unión Europea tienen un gran impacto pero también hay otras cuestiones a nivel mundial. También hay otros principios a nivel mundial que están en consonancia con la Convención 108 de la Unión Europea.

BECKY BURR: Les voy a pedir a todos que, por favor, se identifiquen cuando tomen la palabra.

LUTZ DONNERHACKE: Soy Lutz Donnerhacke, de EURALO. Fui parte del equipo de WHOIS una vez. Estuve en un debate sobre el WHOIS extendido y el WHOIS acotado. Quería enfatizar el hecho de que el WHOIS acotado implica que nosotros hemos entendido que tenemos un sistema legal entendido a nivel mundial. No tenemos problemas con el exceso de datos o con incorporar datos. El enfoque del WHOIS acotado, por otro lado, hacer que las computadoras tomen datos para ubicarlas y para recabar esos datos. dado que nosotros tenemos al WHOIS, si uno le pregunta a un servidor de la IANA, puede hacer una búsqueda especial de un nombre de dominio y puede saber dónde se encuentra pero si uno tiene un enfoque de WHOIS acotado, puede tener también ciertas

respuestas de un registro que diga que vendieron esto al siguiente registrador. Si el registrador tiene datos que han sido recabados directamente del cliente, ustedes pueden proporcionar o dar un servidor de WHOIS a nivel local para que toda la información que sea recabada o que sea brindada nunca abandone el lugar local donde se aplica el derecho originalmente. Tenemos que pensar. Los insto a que piensen en este enfoque porque me parece que es la mejor manera o la manera correcta de hacer esto.

BECKY BURR: Gracias. Quiero agregar algo antes de avanzar. Yo entiendo lo siguiente. Entiendo que la ICANN busca un nombre de dominio, por ejemplo, de un registrante europeo, por ejemplo .COM, y lo va a buscar en el WHOIS extenso pero entiendo que en materia de protección de datos, entendemos que puede haber una transferencia de estos datos. Por ejemplo, de fuera de Europa y que esté sujeto a esos estándares. No estamos seguros de haber eliminado el problema con esta distinción entre el WHOIS extenso y el WHOIS acotado. Simplemente quería comentar eso. ¿Algún otro comentario que quieran hacer?

GIOVANNI BUTTARELLI: Para seguir con este debate de los datos acotados y los datos extensos, quiero decir que todavía no queda muy claro cuál es el

camino a seguir. Por lo tanto, creo que antes de abordar cuestiones en relación a la cantidad de datos, sistemas centralizados versus sistemas descentralizados o los derechos de acceso sobre la base de la legitimidad, no estoy hablando aquí del cumplimiento de la ley. Creo que deberíamos sentarnos y aclarar cuál es el propósito, cuáles son los propósitos, porque para nosotros, francamente hablando, después de que hemos adoptado nuestras opiniones en el 2003, todavía no queda claro por qué es necesario recabar estos datos de una determinada manera, por qué se tienen que publicar de esta otra determinada manera y qué querríamos entender a partir de este propósito. Creo que es necesario identificar una persona de contacto. Tenemos que tener realmente una persona de contacto que esté identificada. Si es así, la tenemos que actualizar en forma constante con respecto a la publicación de estos datos. Es necesario tener una propuesta o una política robusta con relación a estos propósitos secundarios. Creo que, en primer lugar, la primera respuesta a esta pregunta tiene que partir de esto.

BECKY BURR: Le voy a dar la palabra a James y luego a Jim.

JAMES BLADEL: Teniendo en cuenta su sugerencia y en cuanto a debatir los procesos y los propósitos, me parece que este es uno de los propósitos del proceso de desarrollo de políticas del RDS que hemos discutido anteriormente. Es bueno tener este debate de que este trabajo es parte del trabajo base que hay que hacer para poder abordar algunas de estas cuestiones.

JIM GALVIN: Muchas gracias. Yo también quería comentar y enfatizar que cuando hablamos de las diferentes soluciones tenemos que considerar el cumplimiento de los requisitos de privacidad y hacer una diferencia entre las diferentes soluciones que existen. Hay soluciones que tienen que ver con el WHOIS extenso y acotado. Hay que ver cuál de estas dos soluciones es la más adecuada para poder brindar mayores soluciones. Esta es una cuestión, un tema que tenemos que revisar para poder definir nuestros propósitos. Gracias.

BECKY BURR: Adelante.

VITTORIO BERTOLA: Gracias. Soy Vittorio Bertola. Tengo una serie de preguntas pero primero quiero compartir con ustedes mi frustración porque yo no he participado de las reuniones de la ICANN en los últimos

ocho años pero estuve participando anteriormente en la junta directiva y en el ALAC. Hay una serie de cosas que me resultan frustrantes porque siguen igual que hace unos años. El señor Buttarelli fue muy amable al recordar estas cuestiones, cuando se hizo la reunión de la ICANN en Roma. La ICANN, hasta el día de hoy, no ha podido brindar una solución consistente o sólida de por qué estos datos se tienen que recabar. Es un tanto difícil, deprimente, estar aquí y escuchar situaciones o comentarios como los que hemos escuchado en relación a la privacidad y al cumplimiento de la ley. A mí no me gusta ver ningún tipo de actividad delictiva pero no solamente tiene que ver con equilibrar las obligaciones contractuales y la ley, porque no se trata de que la ICANN pueda imponer a la gente determinadas obligaciones o que pueda imponerles a ellos cómo utilizar sus computadoras.

La pregunta básicamente es para el señor Buttarelli y también para las autoridades europeas y para todos aquellos que tienen leyes similares. La pregunta es: ¿Hay algo que se vaya a cambiar, especialmente en el consentimiento informado en Europa? No hemos visto nada en los últimos años. Creo que hemos sido muy pacientes con las autoridades pero necesariamente tenemos que tomar pasos concretos para poder avanzar. Me pregunto si hay algo que vaya a cambiar en relación a este nuevo sistema, al GDRP. No sé quién va a responder a esto pero en el caso de las

autoridades de Europa y en relación a la protección de datos, se envió una carta para que ciertos registros o registratarios dejasen de recolectar y publicar ciertos datos. ¿Los suspenderá la ICANN? ¿Qué hará la ICANN? se tienen que ajustar a la ley. Gracias.

GIOVANNI BUTTARELLI: Vittorio, no estamos aquí para buscar problemas sino para resolver problemas porque somos cuerpos de cumplimiento de la ley. Todos nosotros en 14 meses vamos a comenzar con la exigibilidad. La exigibilidad hace 20 años estaba basada en algo y ahora está basada en otras cuestiones, en penalidades serias. La pregunta es cómo nos vamos a preparar para el día 1, que es el 25 de mayo del 2018. ¿Es todo esto relevante? ¿Se puede aplicar a todo el mundo? En este caso, implica brindar servicios dentro de la Unión Europea. Nosotros no nos vamos a ocupar de los servidores, del establecimiento, de la localización de ciertos servicios, que es básicamente dónde se encuentran los servicios y dónde se ofrecen.

Yo creo que cuando uno construye algo tiene que comenzar desde una estrategia y desde mi punto de vista, la estrategia aquí es el principio de limitación del propósito, que no es el único dentro de la Unión Europea. Es un principio no solamente dentro de la Convención 108 sino que también aparece en otras

convenciones como la convención OECD. Se puede también encontrar en la jurisdicción del tribunal europeo sobre derechos humanos, entre otros. Este es un elemento estable y global. Es un pilar que establece o requiere especificar el propósito. No vamos a buscar un propósito extremadamente detallado. La gente que registra, que brinda la información, piensa al momento de brindar la información que tiene que entender el contexto, el contenido. Esto tiene que ser específico. El propósito tiene que ser específico. Tiene que ser explícito. No tiene que ser ambiguo. Tiene que estar claramente determinado y expresado.

Cuando yo registro estoy sujeto a brindar datos. Tengo que brindar una persona de contacto y básicamente el propósito es la legitimidad. Yo se lo dije. Hace 15 años nosotros estábamos al tanto de la necesidad de garantizar un cierto nivel de transparencia pero luego les pedimos, dependiendo de la identificación de los propósitos, tratar de entender con ustedes la proporcionalidad de la relevancia que tienen las modalidades. En este sentido lo hicimos hace 30 años y preguntamos: ¿Realmente se necesita tener datos extensos versus datos acotados que se publiquen? ¿Hay una alternativa para poder cumplir con este propósito, para lograr todas estas cuestiones de una manera más proporcional?

Me parece que todas estas cuestiones son muy relevantes. Si el problema es el problema de la traducción de los principios, aquí

los podemos ayudar. Antes tuvimos un caso importante pero yo creo que después del mes de mayo de 2018, las autoridades de protección de la ley van a ser responsables de exigir esto en diferentes áreas y también en muchos otros lugares. Esto podría darse en junio, en septiembre, en diciembre del 2018 pero el día finalmente va a llegar.

BECKY BURR: Gail y Joe y Wilbert van a tener también que responder. Luego vamos a cerrar la lista de oradores porque nos estamos quedando sin tiempo. Gail.

ABIGAIL SLATER: Una breve respuesta. Me parece que la razón por la cual este debate nos ha llevado tanto tiempo es porque hay que volver al punto donde tenemos esta cuestión de las acciones o las equidades en competencia. Es decir, hay equidades que se requiere que sean iguales y en este caso el único principio guía son los estatutos. Los estatutos tienen que ver con proteger la resiliencia y la robustez del DNS. Yo no veo que haya equidad en esto. Con respecto a los datos del WHOIS y al cumplimiento con los GDPR y las sanciones y las multas, incluso dentro del ecosistema de la Unión Europea sucede lo mismo. Por esto las empresas necesitan ciertas guías. Hay una obligación competitiva con respecto al comercio electrónico y a las guías

directivas de comercio electrónico que cubren y crean también obligaciones para las compañías que son miembros. Estas obligaciones también tienen que ver con la divulgación de elementos de datos en forma pública. Tenemos que ver si vamos a violar la directiva del comercio electrónico o si vamos a violar por ejemplo las regulaciones que hablan del GDPR.

BECKY BURR: Voy a pedir que las respuestas sean breves. Adelante, Joe. ¿No? Wilbert, adelante.

WILBERT TOMESEN: Voy a tratar de ser breve. A mí me parece que es importante lo siguiente. La pregunta básica es: ¿Por qué nosotros necesitamos procesar estos datos? Es necesario tener una manera que sea menos intrusiva y más inclusiva. La responsabilidad es importante. La responsabilidad para mí significa que me tienen que convencer de que uno va a abordar ciertas cuestiones y que va a asegurar estos datos. Yo le digo a los controladores: "Convénzame de que van a hacer sus mejores esfuerzos". Yo toda mi vida he estado trabajando en exigir esto, en el cumplimiento. El cumplimiento tiene que ver con ser justos y con ser transparentes. Uno puede estar forzado a exigir pero los controladores deben convencerme a mí de por qué lo tengo que

hacer y de cómo lo tengo que hacer y de cumplir los principios que se han establecido. Gracias.

BECKY BURR: Gracias. Vittorio, yo sé que usted está esperando mi respuesta y mi respuesta es que finalmente la ICANN no puede forzar a los registradores y a los registros a elegir entre qué obligación van a querer cumplir o cuál van a aplicar. Adelante, por favor.

MARIA FREDENSLUND: Gracias. Soy Maria. Soy directora de una organización no gubernamental danesa. Trabajamos en Dinamarca con el delito relacionado con las IP. Cuando trabajamos en la exigibilidad o en el cumplimiento de la ley en relación a las actividades delictivas relacionadas con las IP y la protección de productos, nosotros vemos que en este sentido los productos de IP cada vez se utilizan más para un uso delictivo en la cinematografía o en la literatura para poder cometer otro tipo de delitos. Por ejemplo, un sitio web que siempre está registrado en un país extranjero se utiliza para atraer a los consumidores, a los usuarios, para poder instalar malware en sus computadoras con la finalidad de perpetrar otros delitos de naturaleza económica. Los productos de IP se utilizan como un medio para poder obtener tráfico a estos sitios web.

También hemos visto en el último año que ustedes saben que la población danesa es de aproximadamente seis millones y que en el último año hemos tenido más de 200 millones de visitas a este tipo de sitios ilegales que provienen de direcciones de IP danesas. Por lo que vemos, es un problema sumamente importante y que está en crecimiento. Una de las razones de esto es que es muy fácil acceder en forma anónima a Internet. Uno puede establecer un sitio web en un nombre dominio extranjero con una dirección de nombre de dominio extranjero y puede ser anónimo y cometer cualquier tipo de actividad delictiva. Esto constituye un problema sumamente serio.

Mi punto es el siguiente. Por supuesto, necesitamos poder efectivamente hacer cumplir las leyes en Internet. Por supuesto, respetar el equilibrio fundamental de los derechos fundamentales, como por ejemplo la privacidad y otros principios pero, por el momento, el tema o la cuestión es que es muy sencillo ser un delincuente porque no tenemos ninguna forma de interferir con la actividad ilegal, ni siquiera como titular de derecho, como autoridad policial. Una de las razones de esto es que es sumamente fácil estar en el anonimato dentro de Internet. Gracias.

BECKY BURR: Gracias.

GIOVANNI BUTTARELLI: Yo, como miembro del poder legislativo, voy a hablar y también voy a hablar desde mi conocimiento en materia penal. Yo diría que ninguno de los principios de protección de datos evita… A ver, las autoridades de cumplimiento de la ley tienen acceso legítimo y proporcionado a los datos pero ninguna de estas disposiciones evita… A ver, nada de esto evita que el sistema del WHOIS se pueda acceder de manera sencilla. Uno de los temas es la exactitud de los datos. La exactitud de los datos muchas veces se ve como una protección, como una salvaguarda en pos de los datos pero también implica que hay acceso a este tipo de datos. Yo tomo en cuenta sus comentarios. Si el problema es el acceso fácil, en realidad esta es una corporación internacional y en este caso decimos que los principios internacionales no son el problema.

ELLIOT NOSS: Hola, soy de Tucows. Somos un registrador. Estamos en esta organización ya desde hace tiempo. Quisiera comentar que me sorprende mucho este panel. Este quizá puede ser el panel más positivo y optimista en el que he estado en últimos 5 a 10 años. Eso se debe a que hoy en la ICANN nosotros tenemos un desequilibrio. Ese desequilibrio es tal que nosotros los necesitamos a ustedes y a su comunidad para que sean más

activos. Voy a volver al comentario de Thomas sobre las empresas que están en el medio de intereses en competencia. Nosotros hoy en ICANN no estamos siendo apretados entre estos dos sino que estamos siendo empujados por uno de ellos. Estos son la propiedad intelectual y la aplicación de la ley.

Nosotros queremos estar entre esos dos. Yo tengo dos pedidos para ustedes. El primero es que para cada uno de ustedes que empiecen a ser más activos. Ojalá que este panel no sea único y que sea el principio de un lugar permanente dentro de la comunidad de ICANN para que hablen personas que trabajan en la privacidad como ustedes. quiero instarlos a que para el beneficio de cada uno de los miembros del GAC, que estén presentes y que nos den una presión igualitaria a la que hay hoy para los miembros del GAC donde predominante está la aplicación de la ley. Que no sean la aplicación de la ley o los miembros del GAC. Ellos no están lo suficientemente apretados entre una y la otra.

Yo pienso que ICANN tiene que crear una oficina permanente de privacidad. Alguien que tenga verdadero poder porque eso se debe a que la necesidad de esta comunidad es global. Ellos toman en cuenta estos intereses nacionales pero también hay elementos globales singulares a lo que nosotros enfrentamos en términos de jurisdicción, en términos de los mecanismos particulares y de los enfoques específicos. Solamente si la ICANN

da ese paso hacia delante, vamos nosotros a poder ver realmente que hay salvaguardas que cruzan los límites, que cruzan las fronteras y remedios que también cruzan los límites.

BECKY BURR: Creo que tenemos que tener un funcionario de privacidad. El GDPR así lo requiere.

MATHIEU WEILL: Hola. Gracias a todos. Soy Mathieu Weill, jefe ejecutivo de AFNIC, un ccTLD de Francia. También soy proveedor de backend de varios gTLD en Europa. Tengo una perspectiva de la industria. Al igual que Elliot, yo pienso que el futuro es mucho más claro de lo que era antes. Es mucho mejor. Mi comentario es una reacción a lo que dijo James, que es un actor de la industria muy respetado en todo el mundo. Nosotros, como ccTLD, estamos muy preocupados por esta regulación. Lo tomamos muy seriamente y lo hemos hecho desde hace años. Es decir, lo hemos considerado seriamente desde hace años. Creo que lo que nos dice James, si ustedes miran más en profundidad, no está bien expresado. No hay una brecha tan grande entre ser un jugador en la industria de nombres de dominio y estar del otro lado abordando los principios que están en el GDPR.

Nosotros estamos abiertos dentro de la industria y dentro de la GNSO a tener estas conversaciones con los ccTLD europeos también. Hay que compartir cosas para entender exactamente cuáles son las preocupaciones desde el punto de vista de los practicantes porque no son solamente los datos que se deben proteger. Empieza con nosotros y en analizar nuestros procesos. Tenemos que ver exactamente qué significa seguir los principios de estas regulaciones. Al igual que Elliot, nosotros estamos a favor de estos principios. Cuando pensamos en Internet, nosotros los apoyamos y queremos que sea una Internet única, que una a estas personas.

Creo que lo que tenemos que hacer es sobrepasar esta tendencia de decir: “Es una regulación que nos han impuesto y por eso es necesariamente mala”. Nos está llevando en la dirección adecuada. Hay desafíos especialmente para los jugadores globales pero esto se puede resolver si solamente tratamos de encontrar la solución porque esas soluciones han estado presentes desde hace tiempo y las podemos encontrar. Creo que el problema más urgente al que quiero nuevamente instar a ICANN a que mejore sus procesos, a que ayude a los registros y registradores a que cumplan las regulaciones y que no se vean restringidos por los procesos de la ICANN para poder cumplir. Creo que ese es el desafío más grande entre las industrias de las corporaciones y las colaboraciones.

JAMES BLADEL: Creo que Jim quiere responder rápidamente.

JIM GALVIN: Quiero decir que estoy de acuerdo con usted. No creo que se haya dicho poco de que las soluciones empiezan con nosotros. No está exagerado esto. Mi observación tiene más que ver con que nosotros estamos creando un nuevo sistema de gestión de credenciales. Podemos hablar de esto después y durante mucho tiempo pero este sistema es, a escala global, algo en lo que nunca fuimos exitosos en ninguna industria. No tenemos ningún sistema de gestión de credenciales global a escala que pueda validar las identidades, enfrentar a las credenciales, tener acceso en tiempo real a la validación, las credenciales en sí, la operación de este tipo de sistemas. Yo creo que si nosotros avanzamos en esa dirección vamos a tener unos problemas que ninguno de nosotros enfrentó antes a gran escala. Vamos a poder seguir hablando de este tema.

BECKY BURR: Tenemos ahora un foro público que empieza a las 5:00 en punto. Les voy a pedir al resto de la gente que está en la línea que sea muy breve. Vamos a tomar todas sus preguntas y después vamos a tratar de responder rápidamente.

VICTORIA SHECKLER: Estoy aquí en representación del grupo de trabajo de RDS. Tengo una pregunta con dos partes que las voy a leer. Con respecto al cumplimiento del GDPR, la política de consenso de la ICANN tiene que definir un nuevo RDS que permita acceso controlado a los datos de registración. Los datos tienen que tener el consentimiento para que haya un uso legal como la supresión de datos civiles o criminales. También tenemos registratarios que tienen que dar su consentimiento para otros usos y tienen que resolver el debate de los datos de registración que tienen que ser accesibles para el WHOIS. Por ejemplo, los procesos de definición civil y penal. Tenemos un proceso de PDP por consenso que tiene que definir la proporcionalidad y el uso de los datos por parte de terceros o utilizar el consenso como un mecanismo para la proporción legítima. Gracias.

BECKY BURR: Esas son muy buenas preguntas pero voy a decir que, como tenemos poco tiempo, tendremos que responderlas después.

KEITH DRAZEK: Hola. Soy Keith Drazek, de VeriSign. No iba a hacer una pregunta hoy pero las discusiones anteriores entre extendido y acotado hicieron que las quiera plantear. Había un WHOIS ampliado, del

año 2014, que efectivamente requiere que VeriSign nos presente que para los registros .COM y .NET pasemos del acotado al ampliado para recoger datos de 142 de registros de nombres de dominio de nuestros registradores. Muchos de ellos están en Estados Unidos pero otros no. a la luz de la nueva regulación y del paisaje cambiante desde el año 2014, cuando la política de la ICANN se aprobó, a mí me da curiosidad saber si ustedes tienen alguna idea sobre las implicaciones que puede tener la idea de que nuestros registradores tengan que transferir 142 millones de nombres de dominio en un registro. Mirando hacia el año 2018 con la nueva regulación y la posibilidad de un nuevo RDS que se va a implementar, quisiera que tengamos esto en cuenta.

BECKY BURR: Es también una muy buena pregunta pero es una conversación más larga de la que podemos tener. Muy bien. Esto no es algo que se haya terminado. Este es el principio de un diálogo. Quiero agradecerle al Consejo de Europa por plantear y traer estos expertos y recursos a esta sala. Les agradezco a todos por haber venido. Sí, Nigel. Ahí voy.

NIGEL HICKSON: Muchas gracias, Becky. Tenemos que salir de la sala porque tenemos el foro público dentro de nueve minutos.

[FIN DE LA TRANSCRIPCIÓN]