
BARCELONA – HLG M: desafíos temáticos en el ecosistema de la gobernanza de Internet: ciberdelito, protección de datos y privacidad
Lunes, 22 de octubre de 2018 – 12:15 a 13:30 CEST
ICANN63 | Barcelona, España

ORADOR NO IDENTIFICADO: Por favor, no hay pausa para el café. No tenemos tiempo. Vamos a iniciar la sesión ahora mismo.

FRANCISCO POLO: Bienvenidos a todos del *coffee break*. Vamos a pasar a la última sesión de la mañana.

Durante la próxima hora vamos a hablar del ciberdelito, protección de datos y privacidad.

En particular, vamos a hablar de la necesidad de encontrar una forma de diálogo y cooperación para abordar todos estos desafíos que tienen los gobiernos y las personas respecto de la privacidad, la protección de los datos y el aumento en el ciberdelito. También vamos a explorar cómo mantener los derechos humanos y una Internet abierta en un entorno donde hay cada vez más legislación nacional y regional que tiene una influencia conversas.

Ahora le voy a dar la palabra al moderador. Es un placer tener a Awa N'Diaye, presidente de la Autoridad de Datos de Senegal.

Nota: El contenido de este documento es producto resultante de la transcripción de un archivo de audio a un archivo de texto. Si bien la transcripción es fiel al audio en su mayor proporción, en algunos casos puede hallarse incompleta o inexacta por falta de fidelidad del audio, como también puede haber sido corregida gramaticalmente para mejorar la calidad y comprensión del texto. Esta transcripción es proporcionada como material adicional al archivo, pero no debe ser considerada como registro autoritativo.

AWA N'DIAYE: Muchísimas gracias, Sr. Ministro. Si me permiten, voy a hablar en francés.

Voy a empezar inmediatamente agradeciendo al gobierno de España, obviamente, así como a la ICANN, por esta reunión de alto nivel gubernamental. Querría retomar uno de los temas que ya se habló, y que tiene que ver con un tema candente, un tema de actualidad. Ha sido mencionado previamente, y tiene que ver con la seguridad y con la integridad de la Internet en lo que tiene que ver con el ciberdelito.

Nosotros sabemos que la ICANN es el protector técnico, quien garantiza la seguridad en línea. Pero, por supuesto, si bien hay un gran trabajo realizado con la ICANN, desafortunadamente no alcanza para evitar las distintas amenazas que están presentes en la Internet.

En primer lugar, le vamos a pedir a John Crain, quien está a cargo de la seguridad en ICANN, que nos hable de la gobernanza, porque él está a cargo de gobernanza y seguridad. Y es uno de los componentes clave dentro de ICANN para garantizar que la Internet sea abierta, segura y estable.

John Crain tiene la palabra.

JOHN CRAIN: Gracias por darme esta oportunidad.

Quiero hablar un poco casi filosóficamente de lo que es la tecnología y los principios sobre los cuales se diseñó la Internet. La Internet o el ARPANET, como se llamaba anteriormente, suele ser descrita como

algo en evolución. Y lo es. Porque ha cambiado la forma en la que opera nuestra sociedad. Se basó en principios como la ley de Postel, que fue publicada en 1989 por Jon Postel.

El principio es básicamente liberal en lo que acepta y conservador en lo que se envía.

Estos protocolos similares fueron utilizados para desarrollar los protocolos sobre los que funciona la Internet. Además del crecimiento de la Internet, podemos volver a estos principios originales, sobre todo al que tiene que ver con la apertura y la transparencia.

Estas tecnologías o protocolos de la primera época son los que hicieron funcionar la red.

WHOIS, supongo que todos han escuchado hablar de este protocolo, fue parte integral de quienes desarrollaron la red para que pudieran unirse a la red, comunicarse unos con otros y solucionar problemas operativos.

Con el tiempo, WHOIS evolucionó, creció la Internet, se necesitaban más partes interesadas como los registratarios de los nombres de dominios, las autoridades, la propiedad intelectual, los propietarios de marcas, los negocios y las personas.

El principio principal que utiliza el protocolo de WHOIS ha sido siempre el mismo.

La operación estable de la Internet se basa en un concepto básico. Uno no puede operar un sistema descentralizado, e Internet es uno

porque es red de redes -- si no podemos encontrar a la gente que opera esas partes que pueden generar problemas y coordinar respuestas.

Cuando hay fallas en el sistema, usos indebidos, ataques, el acceso a los datos sobre quién es responsable, por que parte del ecosistema, se vuelve crítico para restaurar rápidamente una Internet que opere segura y establemente.

Esto es lo que tiene que ver con la integridad operativa de la Internet.

Podemos hablar de algo simple, como informar que el sitio web tiene problemas, tiene algún contenido malicioso; o puede ser hablar con un proveedor de Internet para decir que hay problemas con nuestro servicio.

Pero la Internet no solo fue revolucionaria, sino que es evolucionaria, porque cambia y evoluciona para adaptarse a las necesidades de los usuarios y de la sociedad. De muchas maneras, la Internet refleja a los usuarios y a la sociedad que la utiliza.

Los principios han cambiado con el tiempo.

Uno de los principios rectores hoy en día tiene que ver, obviamente, con la seguridad.

Y uno de los primeros ejemplos con la tecnología es cuando se agregó seguridad a Internet, que se llama HTTPS. Esto fue desarrollado en 1999, es decir, hace menos de 20 años. Y esta tecnología que ahora nos permite encriptar el tráfico en la web es una de las fuerzas

motoras detrás de la economía digital, porque sin esta forma de encriptado, es muy difícil comprar y vender mercaderías en línea.

En los últimos años hemos visto cómo evolucionó la tecnología para abrazar otros principios. Uno de esos principios es el de la privacidad, que está muy relacionado con la seguridad en muchas formas.

Un ejemplo obvio de todo esto, y supongo que lo han escuchado mencionar, es el Reglamento General de Protección de Datos y la especificación temporaria que fue desarrollada por la ICANN y ahora la comunidad está trabajando en una solución más permanente. Pero este es un factor del ambiente que lleva a un cambio tecnología, donde vemos que el protocolo de WHOIS tiene que adaptarse al protocolo RDAP. Es un cambio de tecnología para generar más privacidad y más seguridad, para adaptar los principios a la tecnología de la Internet.

Esto es normal. Es parte de la evolución de la tecnología.

El RDAP hace años que se está desarrollando. No fue impulsado por el GDPR, sino para incluir más privacidad y más seguridad dentro del ecosistema. Esta es una progresión natural.

Hablamos mucho hoy de qué forma nosotros como comunidad global podemos trabajar en conjunto para adaptarnos a los desafíos y a las oportunidades que nos traen estos cambios. A menudo es un esfuerzo para equilibrar los distintos principios que a veces compiten entre sí cuando generamos una arquitectura.

Seguimos hablando de la solidez y de la apertura, pero también de la privacidad, de la seguridad y de otros principios sobre los que tiene que trabajar la comunidad en pos del beneficio de quienes usan la Internet.

Con esto, les doy las gracias y devuelvo la palabra a la moderadora. Muchas gracias.

AWA N'DIAYE:

Muchísimas gracias, Sr. Crain.

Ya tenemos aquí la base de la arquitectura de esta organización. Usted habló de acceso a los datos. Esta es la palabra que necesitábamos oír. Seguridad sí, por supuesto, pero, ¿cómo podemos preservar la seguridad? ¿Cómo podemos garantizarla? Tenemos que abrir para poder asegurar.

Vamos a dar la palabra a uno de nuestros expertos, quien nos dará otra perspectiva sobre esto. Esta es la perspectiva de la protección jurídica de los datos, la protección de la privacidad de los datos. La parte ética, los derechos inalienables. El señor Enrique Factor, quien representa a la autoridad de protección de datos en España, tiene la palabra.

ENRIQUE FACTOR:

Muchísimas gracias, Madam N'Diaye. Quisiera agradecer a ICANN y al gobierno español por permitirme participar en este foro.

Estuve escuchando a todos los delegados distinguidos. Mi nombre es Enrique Factor. Yo trabajo para la Agencia Española de Protección de Datos, que es la entidad nacional encargada de la protección de los datos. Es parte del Comité Europeo de Protección de Datos. Mi función es la protección de los derechos humanos, sobre todo lo establecido en el artículo 12 de la Declaración Universal de Derechos Humanos, que es similar al artículo 8 en la Carta Orgánica de Derechos Fundamentales de la Unión Europea. Y también en el artículo 18 de la Constitución de España. Tenemos mencionado este derecho, el derecho que todos tenemos de privacidad. Estamos de acuerdo en que todo tiene que ver con los datos. De hecho, nosotros somos datos.

Y los datos que nos definen como seres humanos son los que llamamos datos personales.

Ahora, ¿cómo podemos asegurarnos de proteger los derechos fundamentales? En el mundo real, la policía y otros organismos encargados de la aplicación de la ley se ocupan de esto. Pero, ¿qué pasa en el ciberespacio? En el mundo de las computadoras, estos organismos y las autoridades de protección de datos se unieron en defensa de nuestros derechos.

En la Unión Europea, la privacidad y la protección de los datos no son derechos absolutos, pueden estar limitados en determinadas condiciones según lo establecido en la Unión Europea. El derecho de la privacidad y la protección de los datos tiene que estar equilibrado o ponderado con respecto a otros valores de la Unión Europea, los

derechos humanos, los intereses privados y públicos, como la libertad de expresión, de información, de prensa.

Este derecho a la privacidad y a la protección de los datos también puede contraponerse con otros intereses públicos, como la cuestión de la seguridad nacional.

Los estados miembros de la Unión Europea toman medidas para poder evitar las amenazas y para reforzar las facultades de la policía en mantener la libertad, la seguridad y la justicia. Lo hacemos estableciendo mecanismos de grupo de coordinación de supervisión para una base de datos específica como Eurodac, junto con INTERPOL y Europol. El ciberdelito no es solamente una base de datos para los organismos de aplicación de la ley, hay otras bases de datos como WHOIS que son de gran importancia para combatir el ciberdelito. Pero todas estas deben cumplir con la ley.

Un comentario final. Todos luchamos por la defensa de nuestros derechos, pero esto no puede ser a expensas de la transparencia, la equidad y el cumplimiento con la ley. Muchísimas gracias.

AWA N'DIAYE:

Muchísimas gracias, Sr. Factor. Respetar las libertades individuales, los derechos humanos y las leyes que protegen las libertades individuales. Lo que probablemente me están diciendo es que esto es lo más valioso que tenemos y el derecho más inalienable que tenemos.

Pero hay otra perspectiva, que también es importante. Y es la de la seguridad pública.

¿Cómo podemos nosotros asegurarnos de que estemos protegidos contra la ciberdelincuencia sin que ello tenga un impacto sobre la protección de los datos? ¿Cómo podemos hacer frente a la ciberdelincuencia? ¿Cómo podemos mejorar la cooperación entre los gobiernos y a través de las autoridades de protección de los datos? Para entender esto, tenemos a una persona sumamente calificada que tiene 30 años de experiencia, quien es jefe del Centro Europeo de Ciberdelito, está a cargo de un grupo europeo para definir distintas estrategias en esta área.

Sr. Wilson, tiene la palabra.

STEVEN WILSON:

Muchísimas gracias a las autoridades españolas. Realmente les agradezco que me hayan invitado a hablar ante este auditorio. Les pido disculpas porque había un colega, Tim Morris, de INTERPOL, que iba a hablar también. Pero yo voy a hablar en nombre de las dos entidades, de Europol y de INTERPOL. Estoy aquí para mostrarles la visión estratégica general de los organismos encargados de la protección de la ley y del impacto del WHOIS en nuestras investigaciones y sobre la seguridad pública.

Este es un tema de interés público. ¿Cómo podemos hacer que la Internet sea más segura para todos nosotros? Este es un tema sumamente importante y todos estamos comprometidos con ello.

En primer lugar, con respecto a mi organización, EC3, investigamos todos los ciberdelitos en Europa, más de 200 casos por año en los que trabajamos, sobre todo de fraude, ataques importantes a los bancos europeos, también la explotación sexual en línea, la infantil también, con consultas no solo en Europa sino también a nivel mundial. También trabajamos estrechamente con los colegas de INTERPOL. Y tenemos también una unidad de investigación forense digital que hace todas las investigaciones en una red oscura. Pero también tenemos el terrorismo y el tráfico de personas.

Fíjense en lo que estamos hablando aquí. Agradezco a Enrique por sus comentarios con respecto a la privacidad. La protección y la privacidad de los datos están en el corazón de todo lo que tratamos de hacer nosotros. Es un derecho fundamental. Tenemos aquí que hacer que la Internet sea un lugar más seguro para todos, pero tenemos que lograr un equilibrio entre los derechos de las víctimas, la revictimización de esos niños que han sido abusados, la seria amenaza a la vida que nosotros vemos a diario y la explotación de las personas en línea. Y este equilibrio es difícil de lograr.

Cuando hablamos, nosotros sabemos que no tenemos solamente un conjunto de datos. Si nos fijamos en el GDPR, este es un principio fantástico. Estaríamos mucho más seguros si pudiéramos proteger nuestros datos según los estándares requeridos por esa ley. Sin embargo, creó una consecuencia no intencional para los organismos de protección de la ley y, de hecho, para los tribunales y, en última instancia, para la seguridad pública. No solamente se relaciona con el

ciberdelito, sino también con el contraterrorismo, con el crimen organizado, con el abuso infantil, con los delitos de propiedad intelectual de alto nivel y con el lavado de activos. El WHOIS es el punto de inicio para muchas de nuestras investigaciones. Poder entender los vínculos en las investigaciones es muy importante porque en Internet no hay fronteras nacionales y tenemos que trabajar a nivel internacional. Entonces WHOIS ha sido vital para la velocidad de las investigaciones para algunas de las adversidades más dinámicas que hemos visto en nuestro trabajo.

Les quiero dar algunos ejemplos para darles un contexto de lo que nosotros estamos hablando. Tenemos una investigación de abuso infantil. Este año se organizó un grupo de pedófilos que vendían el acceso a material pornográfico de niños en Internet. Nosotros pudimos recabar información sobre todos los nombres de dominio conectados con este grupo, los sitios web a través del DNS. Es fundamental contar con esta fuente. Por suerte, estos delincuentes cometen errores y nosotros podemos llegar a ellos.

En abril de este año, AMARC, la red de los terroristas de ISIS, trabajando con aliados internacionales, pudieron poner en la red material para reclutar voluntarios para la organización terrorista. Y, una vez más, el acceso a la base de datos de WHOIS fue fundamental para el éxito de esa operación que emprendimos contra ellos en la medida que lo utilizamos, en el caso de la Operación Avalancha hace un año.

El ciberdelito en las redes de servicios, donde hay más de 800000 nombres de dominio comprometidos como resultado de las operaciones de este grupo en esta operación, y esto dio lugar al arresto de cinco personas de alto rango en este grupo. Una vez más, esta consulta no hubiera sido posible si no hubiéramos tenido acceso al WHOIS. Hay muchas investigaciones en curso.

Entonces, damas y caballeros, en el futuro que nosotros visualizamos con un modelo de acceso unificado, vemos que esto es fundamental para lo que tratamos de hacer, una interfaz de usuario única con usuarios acreditados. INTERPOL y EuroPOL trabajan de forma conjunta contra el ciberdelito, y lo importante aquí es poder atrapar a los malos.

Y la velocidad es esencial en estas investigaciones. Los delincuentes desarrollan sus propias autopistas, pero nosotros tenemos que desarrollar las mismas para poder atraparlos y para disuadirlos. Tenemos que asegurarnos de que las bases fundamentales de Internet que todos amamos sean mantenidas, y que esto nos traiga juntos acceso a estas bases de datos entendiendo que el interés público tiene que ser la consideración principal. Muchas gracias.

AWA N'DIAYE:

Muchas gracias, Sr. Wilson.

Yo creo que todos los gobiernos acá reunidos y los miembros del GAC están de acuerdo en que es importante proteger la vida privada de los

ciudadanos, pero también estamos muy preocupados por la cantidad de delitos que vemos en el ecosistema.

¿Cómo podemos terminar esto entonces? ¿Cuáles son las soluciones que podemos encontrar? ¿Quiénes son las partes interesadas que pueden trabajar sobre eso? ¿Cómo podemos garantizar, a nivel de estado, que podemos reducir el debate entre los ciudadanos que están presentes en todas partes? Porque parece que la Internet es el demonio de todos estos delitos. ¿Cómo proteger los datos? Sentimos que es una intrusión dentro de nuestra libertad. Una de las soluciones de las que podemos hablar, y ya hemos empezado hoy por la mañana a hablar de ello, es que uno de los grandes desafíos que enfrentamos es unir a los distintos componentes de la ICANN y trabajar en torno al futuro de la Internet. ¿Cómo podemos construir ese futuro?

Tenemos con nosotros a alguien que es un diplomático que actúa en la sociedad civil y que también es un empresario. Entonces también entiende de la parte técnica. Él generó la Red de Política de Jurisdicción e Internet, o sea que tiene gran experiencia. Y esto es lo que necesitamos dentro de la ICANN para poder trabajar como un sistema de múltiples partes interesadas para llegar a soluciones inclusivas.

Sr. Bertrand de la Chapelle, tiene ahora la palabra. Y creo que quizá nos pueda dar una solución global a todo este tema. Después vamos a escuchar a los distintos países que tienen sus propias perspectivas para hablar de sus expectativas y quizá recibir preguntas.

BERTRAND DE LA CHAPELLE: Es muy bueno ver caras familiares. Quiero compartir algunos puntos. Lo primero es que las tres primeras intervenciones que me precedieron señalaron exactamente cuáles son los desafíos que enfrentamos. Tenemos que reconciliar tres objetivos. Uno es luchar contra los usos indebidos. En segundo lugar, lo tenemos que hacer al mismo tiempo que respetamos el debido proceso y protegemos y alentamos los derechos humanos. Y, en tercer lugar, tenemos que garantizar que el desarrollo de la economía digital sea innovador, no quede atrapado.

Hablo de reconciliar y lo hago adrede, no hablo de “equilibrar”, porque “equilibrar” significa que uno está sacrificando una cosa por otra.

La segunda idea es que todo el tema del WHOIS es una ilustración de lo que está pasando en estas tres dimensiones, porque nos muestra lo difícil que es. Es un debate continuo dentro de la ICANN, y supongo que dentro del contexto del GDPR va a encontrar una solución adecuada.

Pero el tercer punto que quiero señalar es que cuando estamos hablando del DNS a nivel técnico, existe un peligro de verlo como la herramienta final para resolver muchas cosas que suceden en la Internet. Tenemos que ser muy cuidadosos para saber cuál es el rol que pueden tener los operadores del DNS en las diferentes dimensiones.

Cuando estamos hablando de seguridad, de estabilidad y los usos indebidos, como pueden ser el *phishing*, el *malware*, los *bots*, el *software* malicioso, etc. tenemos que pensar en cuál es la posición de cooperación que tienen todos estos operadores del DNS para luchar contra estas cosas.

Ahora bien, cuando estamos hablando del contenido que subyace en términos generales, la capa del DNS no es la herramienta adecuada, porque cuando uno elimina un nombre de dominio tiene un impacto global y el daño o la ilegalidad puede darse a nivel local. Hay situaciones que deben enfrentarse, donde está bien eliminar ese nombre de dominio porque hay un contenido y tenemos un umbral de abuso que ha sido superado. Quería señalar estas dos dimensiones.

Lo que resulta importante -- y yo también trabajé en el Ministerio de Relaciones Exteriores de Francia. A la hora de ejercer la soberanía en la era digital, se encuentran nuevos desafíos. Porque las decisiones que puede tomar un país a nivel nacional pueden tener un impacto en el territorio de otro país. Y es muy importante que cuando se desarrolla la legislación, el impacto que pueda tener esa legislación en otros territorios también sea tenido en cuenta, porque hablamos de comunicación, coordinación y cooperación entre los distintos gobiernos. Lo que resulta más importante entonces es que las decisiones que se toman, y vuelvo circularmente al primer punto, si las tomamos en un silo en particular, en una organización en particular o en un subtema que puede ser economía, tecnología o seguridad, tiene un impacto en los otros desafíos o dimensiones. Y

encontrar esta reconciliación que mencioné al principio es lo que subyace en todo esto.

Entonces, el permitir la cooperación digital, este concepto, debemos considerarlo en distintas dimensiones.

La Red de Política de Jurisdicción, que yo fundé en 2012, tiene tres programas sobre esto. Uno de ellos está directamente relacionado con el espacio de nombres de dominio, pero los otros dos tienen que ver con el acceso transnacional a la evidencia y a las investigaciones penales, que es un desafío transnacional. Además, la gente en la comunidad del DNS quizá no conozca todos los debates que se están dando o que les pueden impactar, por ejemplo, en lo que tiene que ver con la propuesta de evidencia del GDPR.

Otra de las cosas es en qué condiciones puede haber un pedido transfronterizo para sacar determinado contenido de determinada plataforma, como puede ser Facebook, YouTube, etc.

Y lo último es en qué condiciones es adecuado eliminar un nombre de dominio por la actividad que se da dentro de ese dominio.

Eso es lo que nosotros estamos haciendo. Veo que el equipo de cooperación digital está creciendo, porque lo importante es saber qué sociedad digital queremos generar, quién desarrolla las normas, quién las implementa y cómo se adjudican. Muchísimas gracias.

AWA N'DIAYE:

Muchas gracias, Sr. De La Chapelle. El gran desafío que todos enfrentamos no va a resolverse sin los estados. Entonces ahora las

próximas intervenciones de los estados nos mostrarán sus aportes a este pensamiento sobre el papel crítico que desempeñan.

Comenzamos con Uganda, con Frank Tumwebaze, Ministro de Tecnologías de la Información y la Comunicación y Guías Nacionales. Tiene la palabra.

UGANDA:

Distinguidas autoridades y delegados, quisiera comenzar agradeciéndole al gobierno español y a la ICANN por darnos la posibilidad de tomar unos pocos minutos para presentar la postura del gobierno de Uganda, el Ministerio de las TIC.

Aprovechamos esta oportunidad bajo el paraguas de esta reunión gubernamental de alto nivel para poder mostrar nuestra postura sobre algunos temas críticos. Si bien Uganda ha sido miembro durante los últimos seis años del GAC y ha participado en la ICANN, nosotros hemos tenido que solicitar algunas soluciones a la ICANN y realmente hemos felicitado todo el trabajo en pos del interés público y la incidencia que se ha hecho. Pero debemos reconocer que todavía hay mucho camino por reconocer.

Hoy necesitamos considerar el tema de la protección y la privacidad de los datos, que es clave para desarrollar servicios electrónicos en el sector público y privado. Uganda reconoce que esta es una cuestión crítica en la era de la movilidad de los ciudadanos, la naturaleza global de los servicios y los distintos regímenes nacionales en cuanto a la protección de datos.

Esto, a su vez, todavía más complejizado por el distinto grado de capacidades de ciberseguridad que tienen los distintos países y que son miembros de la ICANN. A su vez tenemos los marcos, que pueden tener un impacto sobre el acceso de la información.

Uganda recomienda que el proceso de desarrollo y de aprovisionamiento de las políticas y requisitos gubernamentales que se relacionan con el ecosistema de la Internet, al cual todos contribuimos, debería garantizar que la prestación de servicios públicos y la seguridad nacional no se vean inhibidos.

Estos procesos y estas cláusulas, por lo tanto, deberían tomar conocimiento de los distintos requisitos de interés públicos, los existentes y los que se deberían concebir.

Para concluir, quisiera reiterar el compromiso de mi país, Uganda, para trabajar con las distintas partes interesadas y asegurar el crecimiento continuo y la inclusión del ecosistema de Internet para el desarrollo sostenible de todos. Gracias.

AWA N'DIAYE:

Gracias por ser la precisión, claridad y brevedad, porque quiero recordar a cada uno de los presentadores que solo tienen tres minutos como máximo para hablar. Así que esto fue perfecto.

Ahora le voy a dar la palabra a Pua Hunter, de las Islas Cook, directora de TIC.

PUA HUNTER: Muchísimas gracias. Voy a dar la palabra al representante de Tuvalu, al Ministro de Comunicaciones y Transporte, Monise Laafai. Le voy a ceder mi lugar. Muchas gracias.

MONISE LAAFAI: Muchísimas gracias, damas y caballeros. Mi nombre es Monise Laafai. Soy el Ministro de Comunicaciones y Transporte de Tuvalu. Es mi primera reunión en la ICANN, y es un honor estar acá y representar a mi país.

Muchísimas gracias, distinguido presidente, moderadora y expertos, por darnos su experiencia y sus conocimientos dentro de lo que es el ecosistema de la gobernanza de Internet.

En primer lugar, quiero agradecer fundamentalmente al gobierno de España por la hospitalidad y por esta reunión en esta hermosa ciudad y hermoso país.

Los desafíos que tienen que ver con el ciberdelito, la protección de datos y la privacidad también existen en Tuvalu. Enfrentamos muchos desafíos. Nosotros somos una nación muy pequeña rodeada de océano, y somos vulnerables entonces al cambio climático. También para nosotros es difícil salir del país, y reconocemos que el transporte marítimo es crítico para el desarrollo económico. La alternativa es la telecomunicación y también es muy costosa. Nuestro sector de telecomunicaciones es modesto, es un monopolio porque somos nada más que 11000 personas que se ven respaldadas en nuestra legislación, y ha sido modificada para dar lugar a los

desarrollos electrónicos, al comercio electrónico y para abordar el tema de la ciberseguridad. Es la capacidad entonces de nuestros expertos locales en informática la que resulta limitada en cuanto a las responsabilidades para un gobierno que es multitarea y pequeño. Por ejemplo, nuestro representante de GAC también es el Director Ejecutivo del ministerio de transporte y comunicaciones y se encarga de distintas prioridades nacionales que tienen que ver con la política y con aspectos técnicos. También es quien me asesora como ministro.

A pesar de estos desafíos, estamos embarcándonos en la implementación de un nuevo sistema para comunicar a todas nuestras comunidades en la isla que ha sido financiado por el Banco Mundial. Entonces, este es un desarrollo optimista porque creo que promoverá el desarrollo y la implementación de mecanismos amplios para abordar todos los desafíos que mencioné previamente. Tres minutos no son suficientes para explicar todo lo que hacemos, pero al menos puedo mencionar mi participación en GAC y también decir que queremos cerrar esta brecha digital en mi país y en representación de otros países menos desarrollados. Y también fomentar una comprensión compartida de cuáles son los desafíos que nosotros enfrentamos y cuáles son las mejores prácticas entre los colegas del GAC y la ICANN.

Muchos de nosotros estamos acá escuchando hablar de algunas cosas, pero no sabemos, por ejemplo, cómo puede impactar a nuestro país algunos temas, como GDPR; cuáles son las acciones que se deben tomar, cómo interactuamos con esto. También sabemos que sobre

todo en las regiones del Pacífico es muy difícil venir a las reuniones de la ICANN. Es muy costoso. Y les pido a quienes participan del ambiente de Internet, que fomenten el trabajo de la ICANN en la región, sobre todo para que nosotros también respaldar el trabajo de la ICANN en las áreas de desarrollo de política. Muchísimas gracias por estos minutos.

AWA N'DIAYE:

Muchísimas gracias. Ahora damos la palabra a la República Dominicana, el Sr. Nelson Guillen, miembro de la junta de INDOTEL.

NELSON GUILLEN:

Me gustaría comenzar agradeciendo, en nombre del gobierno dominicano, al gobierno español por acogernos en la bella ciudad de Barcelona para esta reunión. La República Dominicana se ha comprometido a establecer los mecanismos adecuados de ciberseguridad para proteger a las instituciones del estado, sus ciudadanos y los sectores productivos. Estas medidas buscan garantizar el desarrollo confiable de las actividades de toda la población en un marco de respeto a los derechos humanos.

Sin embargo, hemos visto cómo para enfrentar a grupos fundamentalistas que a menudo utilizan Internet para la propaganda y el reclutamiento, varios gobiernos han promulgado leyes que aparentan combatir la ciberdelincuencia y el ciberterrorismo, pero que terminan utilizándose para reprimir la disidencia. Es preocupante que la seguridad nacional, el ciberdelito e incluso conductas como la

difamación o la injuria en algunos casos sirvan de excusa a legisladores para criminalizar explícitamente a los que critican la legitimidad de un gobierno o para atacar y reprimir el discurso político crítico. Consideramos que perseguir, enjuiciar y encarcelar a los usuarios de Internet por expresarse de manera efectiva, restringe el discurso crítico, pero al mismo tiempo descuida la creación de una solución integral que pueda hacer frente a largo plazo a la amenaza de los movimientos terroristas. Nos preocupan las propuestas de leyes que utilizan el mantra de la ciberseguridad para argüir una mayor apertura de los datos de WHOIS pero cuyas implicaciones van en pos de beneficiar intereses particulares. Esto se traduce en un claro conflicto de interés que debe resolverse a nivel global y que ICANN puede contribuir a esta solución. La República Dominicana, en su interés de contribuir a la mejora de la conectividad global de Internet y en apoyo a los derechos individuales, a la privacidad y a la libertad en Internet, rechaza este tipo de intervención en la gobernanza global de Internet, pues el interés general debe siempre imponerse sobre intereses particulares. Muchas gracias.

AWA N'DIAYE:

Muchas gracias. Le voy a dar la palabra a la Comisión Europea, al Sr. Pearse O'Donohue, Director de Redes del Futuro de la Comisión Europea, DG Connect.

PEARSE O'DONOHUE: Muchísimas gracias. La legislación europea, el GDPR que se ha mencionado como un ejemplo clave, se está moviendo en esa dirección. Enrique Factor habló de esta legislación y la puso en contexto, que tiene que ver con la protección de la privacidad en general así como con otras consideraciones de política pública. No voy a entrar en detalles. Pero tenemos delincuencia y además amenazas a la seguridad que los organismos de aplicación de la ley tienen que evaluar. Claramente, necesitamos acceso a la información necesaria.

Hay un equilibrio entonces entre mantener la privacidad y asegurar que se cumpla con la ley y se proteja contra estas amenazas cibernéticas. Pero como dijo Bertrand de la Chapelle, no se trata de elegir uno u otro, sino que es una paradoja. Para poder proteger una Internet abierta y al mismo tiempo alimentarla, que es la misión, así como un vehículo para todos, para beneficiarse económica y socialmente, para proteger los datos de la gente y para confiar en la Internet para que la gente participe, actúe en Internet y se beneficie de ella, para lograr todo eso, nosotros también debemos garantizar que la Internet sea segura, sea confiable y que no sea un lugar donde se permite el delito. Y esa paradoja, ese equilibrio, es el que debemos buscar de forma constante.

Se mencionó una y otra vez el trabajo del GAC y también de la comunidad de la ICANN, incluso durante esta reunión. Quiero hablar específicamente de lo que tiene que ver con su impacto en el WHOIS. Y he escuchado también otras intervenciones sobre temas más amplios,

pero lo que puedo decir es que todos los países miembros de la Unión Europea y la Comisión Europea opinan lo siguiente. La Unión Europea entiende cuál es la responsabilidad de la ICANN para garantizar la seguridad, la estabilidad y la flexibilidad del sistema de nombres de dominios. Y como parte de esa función, la ICANN debe garantizar el funcionamiento del sistema del WHOIS, que incluye la recopilación, el almacenamiento y a veces la entrega de datos precisos que tienen que ver con los registratarios. Tiene que haber una protección completa de los datos de miembros de la Unión Europea, así como el cumplimiento de las leyes de otras regiones.

Nosotros respaldamos el diálogo continuo entre la ICANN y las autoridades de protección de datos europeos, que también están acá presente, y que son entes reguladores independientes. No están sujetos a ninguna influencia gubernamental. Lo que tenemos que hacer es garantizar el respeto de todas estas normas. También debemos subrayar que en ningún lugar del lugar GDPR no hay nada que detenga el tratamiento de los datos para objetivos legítimos, como puede ser la aplicación la ley, la ciberseguridad o la protección de derechos de propiedad intelectual. Se trata de identificar cuál es ese objetivo legítimo y encontrar un equilibrio entre las necesidades legítimos y la protección de los datos individuales. Nosotros creemos que esto va a ser de mucho beneficio para la ICANN, para toda la gobernanza de Internet. Es una tarea difícil, pero sin lugar dudas va a ser muy útil en el futuro porque va a proteger uno de los temas fundamentales, uno de los derechos fundamentales, que sé que todos

los gobiernos están comprometidos con él, pero también que la Internet pueda trabajar en su máxima expresión en el futuro. Gracias.

AWA N'DIAYE:

Muchas gracias. Le voy a dar la palabra ahora al gobierno de la India, al Dr. Gulshan Rai, quien es coordinador de ciberseguridad a nivel nacional.

GULSHAN RAI:

Gracias, Sra. Moderadora. Le agradezco la oportunidad a la ICANN y al gobierno de España por permitirme hablar en este foro. La economía digital está creciendo rápidamente. Nosotros esperamos llegar a tener para el año 2022 muchísimo crecimiento de la economía.

Junto con el crecimiento de las telecomunicaciones, que también es algo que está surgiendo -- el ciberdelito, la ciberseguridad, la privacidad, la libre circulación de la información, han sido tratados aquí como temas de gran importancia. El desarrollo de este marco de privacidad ha sido anunciado por el ministro en su mensaje, y nosotros tenemos una política y una estrategia sobre ciberseguridad, que realmente es muy interesante. Sin embargo, vemos todavía un desafío, no solamente para la India sino para todo el mundo en este ámbito. No podemos tener distintos marcos a nivel mundial que no sean compatibles. Algunos marcos anunciados recientemente han ocasionado algunas dificultades y algunas de ellas ya han sido mencionadas en otra de las intervenciones por algunos de los expositores en este panel.

El 90% de los ciberdelitos hoy en día son de naturaleza internacional, y un 10% corresponde al nacional. Sin embargo, esta cifra puede ir cambiando. Junto con el gobierno, la industria va a tener que desempeñar un papel para poder lidiar con los problemas que resultan de la ciberseguridad y el ciberdelito.

Si hoy nos fijamos en el mapa mundial, vemos que hay fronteras específicas y algunas soberanías. No hay fronteras para los delincuentes que trabajan en todo el mundo. Los operadores también trabajan de una manera fluida, interconectada, con redes interoperables que manejan todo el tema de la ciberseguridad, la privacidad y la libre circulación de información. Es sumamente importante contar con una Internet segura, y la India está comprometida a trabajar en este marco interoperable que permita tener en cuenta todas las cuestiones emergentes en esta área. La inteligencia artificial, *big data* y el aprendizaje automatizado están desempeñando un papel sumamente importante. La ICANN, y en particular el GAC, tienen un papel clave que desempeñar para que estas comunidades se unan para lograr un marco interoperable y para resolver los problemas que están surgiendo tan rápidamente. Muchas gracias.

AWA N'DIAYE:

Voy a dar la palabra a Estados Unidos con el Sr. David Redl, que es su Secretario de Comunicaciones e Información y Administrador de la NTIA.

Tiene tres minutos como máximo. Gracias.

DAVID REDL:

Gracias por esta oportunidad para hablar de varios temas. Estados Unidos obviamente apoya el modelo de múltiples partes interesadas. Es un proceso de consenso ascendente que favorece a este ecosistema. Nosotros incluimos dentro del ecosistema a distintos temas, que incluyen la privacidad, la ciberseguridad y un apoyo a lo que es el modelo de la ICANN.

Los desafíos de la gobernanza de Internet colectivamente que estamos enfrentando no son fáciles de resolver. Y vamos a tener que tomar decisiones también a nivel de la NTIA. Todo el mundo se puede beneficiar de este apoyo, porque los innovadores van a poder generar una Internet más segura, más próspera y más innovadora. Este es un desafío, cómo preservar el acceso a los datos del WHOIS mientras manejamos la implementación del GDPR. Saben que el servicio del WHOIS es una gran herramienta para los objetivos legítimos de la ciberseguridad, protección de derecho de propiedad intelectual y autoridades de aplicación de la ley. Sirve también para aplicar la estabilidad, la seguridad y la confianza en el DNS, así como proteger los datos individuales, si bien los funcionarios de Europa, sobre todo la Comisión Europea de Protección de Datos, han confirmado la importancia del acceso a WHOIS, también la ICANN ha sancionado una especificación temporaria y los miembros de la comunidad de la ICANN están trabajando arduamente para que esto se transforme en una política definitiva a través de un EPDP. Esto nos habla también del

riesgo de quienes proveen servicios de DNS, porque tenemos distintas variabilidades entre las empresas para ver cuál puede ser la solución adecuada.

Es por eso que Estados Unidos apoya la participación de la organización ICANN junto con los colegas de Europa para simplificar entonces este desafío de cómo tener acceso y generar un modelo de acceso unificado a los datos del WHOIS. Sabemos que la especificación temporaria va a vencer en breve, y sé que el GAC está tomando un rol activo dentro de la comunidad. Y Estados Unidos está listo para trabajar con los colegas del GAC para lograr esta resolución definitiva. Gracias.

AWA N'DIAYE:

Ahora le voy a dar la palabra a Malasia, al Dr. Mohd Ali Mohammad, Secretario General del Ministerio de Comunicaciones y Medios.

MOHD ALI MOHAMMAD:

Voy a ser muy breve.

Dados los acontecimientos actuales y los cambios en la tecnología, los organismos encargados de la aplicación de la ley en Malasia están enfrentando numerosos desafíos nuevos al combatir los delitos en la era de la convergencia. Los delincuentes se están volviendo más sofisticados mientras que los métodos convencionales de investigación tal vez ya no puedan ser tan eficaces como antes.

Para poder abordar estos desafíos, los organismos de aplicación de la ley en Malasia utilizan toda la información que está disponible y que puede ayudar en el proceso de investigación, incluida la información del WHOIS. Los organismos encargados de la aplicación de la ley a través de canales con base jurídica también piden la asistencia de los administradores de nombres de dominio para que provean información relacionada con las investigaciones.

Por ese motivo, el papel del sistema de nombres de dominio y la comunidad de WHOIS son cruciales y deberían retenerse a la luz de las necesidades de los organismos de aplicación de la ley y las investigaciones. Muchísimas gracias por darme la palabra.

AWA N'DIAYE:

Gracias por ser breve. Como tengo más tiempo, le voy a dar la palabra a John Crain, porque nosotros estuvimos hablando de los nombres de dominio y WHOIS y quizás él nos pueda dar información adicional al respecto. Gracias.

JOHN CRAIN:

Gracias. Si me permiten, escuché hablar mucho del WHOIS y de lo importante que es la base de datos de WHOIS. Y quiero aclarar, para quienes no asistieron a la sesión técnica de ayer, que cuando hablamos del WHOIS o cuando hablamos del RDAP, que va a ser el reemplazo del WHOIS, son sistemas descentralizados. No existe una base de datos, sino que existen muchas bases de datos en distintos

lugares del mundo. Y este es un elemento importante que tenemos que tener presente.

Creo que es excelente tener estos debates acá en la ICANN porque están todas las partes reunidas, se debaten soluciones, se habla de los principios que tienen que ver con la seguridad, la privacidad y la solidez de la red.

Y ahora le devuelvo la palabra a la moderadora. Gracias.

AWA N'DIAYE:

Muchísimas gracias, Sr. Crain.

Ahora voy a dar la palabra a México con el Sr. Víctor Lagunes Soto Ruiz, quien es el jefe de la Unidad de Innovación y Estrategia Tecnológica de la Presidencia de la República.

VÍCTOR LAGUNES SOTO RUIZ: Gracias a España y a la ciudad de Barcelona, y a ICANN por su continua colaboración y cooperación en temas de digitalización y de gobernanza de Internet.

El rol de México obviamente en temas de digitalización ha sido uno muy ambicioso, ha sido uno en donde la estrategia digital de conectividad ha sido muy fuerte. Y mientras vamos conectando más y más mexicanos y cerrando la brecha digital, también estamos más expuestos en temas de cibercriminalidad, así como preocupación por temas de privacidad y datos personales.

Desarrollamos la estrategia nacional en materia de ciberseguridad en colaboración con todo el ecosistema, en un ambiente de múltiples partes interesadas. El año pasado pudimos publicar esta estrategia en colaboración con no solo la industria y el sector técnico, académico y social-civil, sino también observadores y expertos internacionales en colaboración con la ONU, con UNESCO, con la Organización de Estados Americanos, en donde esta estrategia nos ayuda a fortalecer mucho en temas de digitalización pero también en temas de protección de los ciudadanos para proteger la sociedad y los derechos, para poder proteger nuestra economía y la innovación. Instituciones públicas, seguridad pública, seguridad nacional, a través de programas de concientización, programas de creación, de fortalecimiento de una cultura de ciberseguridad, creación de capacidades, coordinación y colaboración con el entorno. Investigación y desarrollo, establecimiento de criterios técnicos y estándares, así como protección de infraestructuras críticas, fortalecimiento de marcos legales. Todo esto para establecer lineamientos en aras de fortalecer un desarrollo sostenible en Internet.

Me da mucho orgullo compartirles que WSIS, *the World Society of Information Society*, ha nombrado la estrategia nacional de ciberseguridad de México como un *champion* el año pasado. Gracias.

AWA N'DIAYE:

Muchas gracias. Ahora le voy a dar la palabra a Brasil, al Embajador Benedicto Fonseca Filho, quien es director del Departamento de Ciencia y Tecnología.

BENEDICTO FONSECA: Muchísimas gracias. Quisiera brevemente hacer referencia a la importancia que le asigna el gobierno brasileño al nexo que existe entre el ciberdelito, la protección de los datos y la privacidad de estos. Es un tema prioritario para nosotros.

En agosto, nuestro país aprobó una nueva ley sobre protección de datos inspirada en gran medida por el GDPR. Esta ley entrará en vigor en febrero del 2020. También estamos discutiendo y elaborando una estrategia de seguridad a nivel nacional. Y también a nivel mundial hemos estado defendiendo fuertemente el derecho a la privacidad en la era digital. Hemos estado patrocinando resoluciones junto con Alemania, promoviendo estas resoluciones en el contexto de las Naciones Unidas. Tenemos también maneras de buscar instrumentos para luchar contra el ciberdelito.

Esto es simplemente para ilustrar y voy a hacer referencia a una noción que fue mencionada por Bertrand de la Chapelle, la importancia de la comunicación, la cooperación y la coordinación entre los gobiernos dentro de la comunidad internacional para poder tratar todas estas cuestiones. En ese contexto también escuché a Bertrand decir que el debate en torno al WHOIS ilustra las tres dimensiones que nosotros queremos lograr, luchar contra el abuso, proteger los derechos humanos y no socavar el desarrollo en el uso de las tecnologías digitales.

En este contexto, también quisiera resaltar la importancia de la red de Internet y jurisdicción, que nos da una plataforma para la discusión de estas cuestiones porque no tenemos un lugar a nivel local entonces esta red nos permite abordar las cuestiones de jurisdicción en esta discusión. Creo que esta provee un espacio muy importante para eso.

Y, por supuesto, esperamos con ansias participar en las discusiones sobre el WHOIS en el contexto de la ICANN y entendemos que debemos encontrar un equilibrio correcto para satisfacer las preocupaciones en términos de la privacidad de los datos, pero a su vez también las necesidades de las entidades como INTERPOL, que tienen la urgencia de utilizar estos datos. Hemos escuchado a otros colegas brasileños también hablar sobre este tema, y hay un interés claro para conciliar las distintas dimensiones de la manera apropiada. Gracias.

AWA N'DIAYE:

Gracias. Ahora voy a dar la palabra a Samoa. Va a hablar Afamasaga Lepuiaí Rico Tupaí, Ministro de Tecnologías de la Información y Comunicación.

AFAMASAGA LEPUIAÍ RICO:

Sra. Moderadora, querría dejar pasar esta oportunidad y hacer mi presentación más adelante. Gracias.

AWA N'DIAYE:

Sí, por supuesto.

Ahora le voy a dar la palabra entonces a Suiza, Niklas Nilsson, que es el Primer Secretario de la Embajada de Suecia en España.

NIKLAS NILSSON:

Gracias por esta oportunidad de permitirnos expresar la visión sueca respecto de los derechos humanos.

Nosotros cuando hablamos de derechos humanos y las TIC en general o lo que es los derechos humanos, nosotros sabemos que los derechos humanos son fundamentales y se aplican en línea y fuera de línea. Tienen que ser respetados y tienen que ser garantizados por los estados, que son los que guían los estándares globales para el ciberespacio. El respeto para los derechos humanos en la Internet realmente está decayendo. En los últimos años, muchos gobiernos, incluso las autoridades que se vinculan con las políticas públicas, han visto censurados ciertos contenidos en línea. También se ha utilizado la Internet para propaganda y desinformación. Y estos límites restringen la participación de los ciudadanos en la sociedad y además limita los hechos fundamentales de la democracia.

Esta tendencia se ve en el contexto global, y hay cada vez más regulación opresiva que no solo limita la libertad de expresión, sino también la posibilidad de que los ciudadanos participen en la vida democrática. Damas y caballeros, gracias a Internet y a las redes sociales, ahora la Internet y los derechos humanos son más conocidos en todo el mundo que anteriormente.

Este rol positivo de las TIC en nuestras vidas, en la democracia y en la economía debe ser resaltado. Y este es un relato positivo de que la Internet debe mantenerse. La Internet tiene un gran potencial para promover el desarrollo económico y generar un entorno facilitador para sociedades diversas, inclusivas y democráticas. La capacidad de unir a la gente y a los políticos, acercarlos unos con otros, no debe ser limitada. Ni limitar la libertad de la Internet, porque es limitar nuestro propio desarrollo. Entonces, nosotros sostenemos que el elemento de los derechos humanos tiene que estar presente en todos los debates, en todas las oportunidades y en todos los desafíos que tienen que ver con la digitalización.

El modelo de múltiples partes interesadas, con actores que provienen del gobierno, de la industria y de la sociedad civil, incluso los que defienden los derechos humanos, es clave cuando estamos hablando de desarrollar un marco, unos contenidos y unas normas comunes para la Internet.

Entonces, quiero repetir la ambición de Suecia de una Internet que sea abierta, libre y segura, con acceso igualitario e inclusiva para todos. Gracias.

AWA N'DIAYE:

Ahora le quiero dar la palabra a Países Bajos, si no me equivoco. El Sr. Geert Moelker, miembro del Consejo para la Economía Digital en el Ministerio de Economía y Clima.

GEERT MOELKER:

Voy a tratar de ser breve. Quiero referirme a dos cuestiones vinculadas con el WHOIS. Se ha dicho mucho acerca de conciliar o de equilibrar los distintos derechos fundamentales vinculados con la privacidad, pero también la necesidad de proteger del crimen. Y consideramos que no es una concesión recíproca la que hay que hacer, sino que hay que resolver esta cuestión del equilibrio, y si una organización en la que esto se puede hacer, es justamente la ICANN porque tiene tantas múltiples partes interesadas, tenemos una posición singular para poder hacer eso en este ámbito.

Mi segundo comentario tiene que ver con la urgencia. Estamos aquí enfrentando la necesidad urgente de encontrar maneras para acceder a los datos del WHOIS. Desde mayo de 2018, muchos registros han modificado el acceso al WHOIS. Lo han hecho por cuenta propia, sin mucha coordinación. Si nosotros no tenemos un modelo armonizado, la fragmentación va a seguir empeorando. Las entidades encargadas de la aplicación de la ley van a seguir encontrando obstáculos en sus investigaciones, mientras que los usuarios no van a tener certidumbre sobre cómo se están guardando de manera segura sus datos personales. Una vez más vemos el rol pivotal de la ICANN. La ICANN es la única organización a nivel mundial que puede dar un abordaje uniforme para ello.

La reforma del WHOIS no puede quedar sin solución. Necesitamos soluciones oportunas. Claramente, esto trasciende del proceso de políticas que nosotros conocemos con el sistema de nombres de dominio. Requiere la colaboración de la junta directiva, de la ICANN

en sí misma y de otros interesados, tanto dentro como fuera de la ICANN. Apoyamos el modelo de múltiples partes interesadas, pero también, en mi opinión, el debate sobre WHOIS es un nuevo caso testigo para este modelo después de la transición de la custodia de las funciones de la IANA, entonces asegurémonos de aprobar este examen.

Gracias.

AWA N'DIAYE:

Muchas gracias.

Ahora voy a dar la palabra a la última oradora, Rita Forisi, Directora General del Instituto Superior de Comunicaciones y Tecnologías de la Información.

RITA FORISI:

Distinguidos delegados, damas y caballeros, en primer lugar quiero agradecer al gobierno de España por ser el anfitrión de esta reunión gubernamental de alto nivel. Nosotros sabemos que el WHOIS es una guía que está abierta a todos pero que ya no puede ser accedida por todos.

Los datos del WHOIS se utilizan para diferentes objetivos, incluso para objetivos de política pública. Por ejemplo, los que tienen que ver con la aplicación de la ley, iniciativas de ciberseguridad, mecanismos de protección de derechos de propiedad intelectual. Y esto es lo que se llama el entorno global de nombres de dominios.

Italia respalda entonces las tareas realizadas para soluciones permanentes, pero también queremos enfatizar que tenemos que acelerar la investigación de un modelo de acceso global que sea aceptable por todas las partes involucradas.

Tenemos que encontrar una solución global para equilibrar los distintos intereses y ese tiene que ser un objetivo alcanzable. Para tener éxito, nosotros tenemos que seguir cooperando entre todas las partes involucradas dentro de la comunidad del sistema de nombres de dominio. Al mismo tiempo, toda la comunidad del DNS debe reconocer que actuar rápidamente es una de las cosas que nos preocupa cuando hablamos de los temas de la gobernanza de Internet. Italia cree que un dialogo continuo entre la ICANN y las autoridades de la Unión Europea resulta esencial. Todos estamos enfrentando el mismo desafío, que es proteger al mismo tiempo todos los temas mencionados acá que tienen que ver con este modelo de múltiples partes interesadas de la Internet.

Gracias.

AWA N'DIAYE:

Muchísimas gracias.

Acá llegamos al final del debate con los diferentes estados. Podemos ver que no tenemos temas que se enfrentan sí ni entran en conflicto, sino que se toman en conjunto. Es algo necesario. Necesitamos escuchar estos principios fundamentales de derechos humanos.

También existe la necesidad de que todas las partes interesadas de ciberseguridad hablen entre ellos.

Y antes de terminar con este panel, querría volver al Sr. De la Chapelle para que nos diga nuevamente lo importante que resulta encontrar una solución global, una solución de múltiples partes interesadas.

Tiene un minuto.

BERTRAND DE LA CHAPELLE: Creo que se trata menos de una solución global que de identificar cuáles son los problemas tema por tema, porque yo escuché varios temas. Sobre el tema de WHOIS, hay una clara conexión entre lo que se debatió en el primer panel, que es cómo se da la interacción entre los gobiernos y el resto de la comunidad, que se da dentro de la ICANN, y cuánto los gobiernos que participan en el GAC también están transmitiendo lo que se debate en sus propios procesos.

La segunda idea que quiero señalar es, en la medida en que la ICANN sea un espacio importante, también hay que reconocer que tiene un área de incumbencia limitada, porque todo lo vinculado con la Internet tiene una tendencia a caer dentro de esta comunidad. Tenemos que identificar entonces dónde se manejan los temas, tema por tema, en lo que tenga que ver con innovación de política, porque hay algunos temas que no le pertenecen a la ICANN, entonces tenemos que generar nuevas oportunidades fuera de ella. Hay temas nuevos que están surgiendo para esta comunicación, cooperación y coordinación entre los distintos actores.

Entonces creo que no hay una solución global, sino un enfoque global a la innovación política para hablar tema por tema y que los distintos actores se reúnan, porque acá se hacen algunas cosas pero hay otros que están haciendo cosas similares también.

AWA N'DIAYE:

Muchas gracias, Sr. De la Chapelle.

Para concluir, le voy a dar la palabra nuevamente al Presidente. Querría recordarles a todos lo importante que resulta todo esto. Tenemos que reforzar la cooperación entre las distintas partes interesadas. El modelo de múltiples partes interesadas resulta esencial para llegar a una solución, aunque esa solución sea compleja, como se mencionó.

Otra cosa importante que quiero recordarles y que se mencionó en esta sesión es que tenemos que armonizar las leyes. Tenemos que hacerlo para llegar a la solución. Las leyes nacionales no tienen que estar unas contra las otras, sino que tiene que haber una oportunidad para no desviarse de esta libertad de expresión en la Internet, para que se pueda confiar en la Internet, para que la Internet sea beneficiosa para todos.

Muchísimas gracias. Le doy la palabra al Sr. Presidente.

FRANCISCO POLO:

Muchísimas gracias. Ha sido una sesión excepcional. Quiero dar las gracias a todos los que hablaron.

Este es el final de la mañana. Volveremos las 15:00 para la segunda parte de esta reunión.

Muchas gracias.

MANAL ISMAIL:

Muchísimas gracias, Sr. Presidente. Muchas gracias a la moderadora, los expertos en la materia, los oradores y a todos los representantes de las delegaciones.

Como mencionó Francisco, este es el almuerzo para los jefes de delegación que tienen el *sticker* naranja. Por favor, vayan al salón de banquetes. Pueden tomar las escaleras que están aquí a la salida, sigan los carteles y van a ser guiados por el personal de la ICANN. Para todos los demás, disfruten de su almuerzo y asegúrense de volver a la sala a las tres de la tarde. Muchas gracias.

[FIN DE LA TRANSCRIPCIÓN]