ICANN69 | Reunión general anual virtual – Sesión sobre políticas de At-Large: más allá de Budapest: el Convenio de las Naciones Unidas sobre ciberdelincuencia y el uso indebido del DNS
Martes, 20 de octubre de 2020 - 16:30 a 17:30 CEST

MICHELLE DESMYTER: Vamos a comenzar esta sesión. Por favor, demos inicio a la grabación. Gracias. Hola y bienvenidos a esta sesión de política de At-Large: El convenio de Budapest sobre la ciberdelincuencia. Soy Michelle Desmyter. Voy a ser quien gestione la participación remota. Tengan en cuenta que esta sesión se está grabando y se rige por los estándares de comportamiento esperado de la ICANN.

Durante esta sesión, las preguntas o comentarios solo se leerán en voz alta si se envían en la forma correcta. Va a haber preguntas y comentarios durante el tiempo establecido para esta sesión. La interpretación para esta sesión va a incluir español y francés. Se va a realizar utilizando Zoom y la plataforma de interpretación remota operada por Congress Rental Network. Se invita a los asistentes a descargar la aplicación de Congress Rental Network siguiendo las instrucciones del chat o del documento que está disponible en la página de la reunión.

Si quieren hacer una pregunta o comentario, levanten la mano. Cuando digan su nombre, activen su micrófono. Mencionen su nombre para los registros y el idioma en el que van a hablar si es que no hablan inglés. Al tomar la palabra, por favor, hablen a una velocidad

razonable para permitir una interpretación correcta. Silencien su micrófono cuando no estén hablando. Recuerden también silenciar todos sus dispositivos, incluida la aplicación de CRN. Con esto le doy ahora la palabra a Joanna Kulesza para comenzar.

JOANNA KULESZA: Muchas gracias, Michelle. Gracias por participar de esta sesión. Tengo unas diapositivas. Si las podemos poner en la pantalla. Les voy a presentar a los oradores. El título de esta sesión, como está indicado en nuestra agenda, iba a ser un poco controversial. Estamos pensando en más allá de Budapest y el presidente de la Convención de Budapest iba a estar aquí. Lo hace todavía más controversial. Hablamos de más allá de Budapest para pensar en cuáles son los procesos internacionales legislativos actuales y futuros que están apuntando a las actividades maliciosas online. Aquí, dentro de At-Large, nosotros hemos realizado varias sesiones y hemos tratado de hacer participantes activos de las conversaciones que están ocurriendo dentro de la ICANN sobre el uso indebido del DNS.

Tan ambigua como suena la sesión para una persona que no pertenece a ICANN, nosotros conversamos sobre el uso indebido del DNS y At-Large le ha dedicado muchos esfuerzos a generar capacidades sobre el uso indebido del DNS. Esta sesión es otro intento de que podamos entender mejor qué significa el uso indebido del DNS y cómo proteger a los usuarios finales efectivamente. Tratamos de analizar instrumentos existentes que quieran lograr la misma meta y

también vamos a analizar posibilidades futuras para que el uso indebido del DNS se convierta en un tema para la totalidad de la comunidad. Si podemos pasar, por favor, a la próxima diapositiva. Estas son muy básicas.

Aquí tenemos la agenda y una introducción de lo que vamos a ver. Voy a comenzar con un resumen de las conversaciones que tuvimos aquí en At-Large donde hemos analizado las distintas tendencias geopolíticas que se centran en las políticas internacionales que pueden tener un impacto en la comunidad de la ICANN. También hemos analizado el trabajo de la ONU y les voy a dar una breve introducción y un marco sobre el lugar en el que nos encontramos en este contexto geopolítico.

Luego, nuestro colega de EURALO nos va a dar una perspectiva de usuario final. Matthias aceptó ser el caso de ejemplo de los usuarios finales para enfrentar las políticas que el uso indebido del DNS puede traer. Finalmente, como dije, estoy muy contenta de que Alexander Seger haya aceptado participar hoy de esta sesión. Vamos a tener solo 60 minutos y hemos reservado una parte importante de ese tiempo para la discusión y el debate. Espero que Alexander nos pueda dar unas ideas de las similitudes entre las políticas del DNS y los procesos internacionales existentes y futuros que apuntan a lo mismo. Es decir, que los usuarios de Internet estén seguros.

Voy a pasar a la siguiente diapositiva para mostrarles cuál es el contexto y de qué se trata esta conversación. Lo siguiente es obvio

para todos los que han participado de las reuniones recientes de la ICANN. Seguimos hablando del marco del uso indebido del DNS que es un documento de política que ha sido desarrollado por aquellos que están en la línea de frente de la lucha contra el uso indebido online. Aquí vemos la definición del uso indebido. Esto es algo que ustedes van a encontrar también en el marco y algo que yo sé que mis colegas y distinguidos invitados están esperando ver.

Tenemos algunas actividades que están definidas como dañinas para la red, uso indebido del DNS. Por lo tanto cubre nociones como malware, botnets, phishing, farming y cómo hemos explorado dentro de At-Large el más controversial, más polémico spam. Vamos a ver también una definición más específica, si podemos ver la siguiente diapositiva.

Aquí hay una definición más específica del uso indebido del DNS y de las acciones que se esperan de los registros y registradores al intentar lograr que la red sea segura. Como verán hay una forma de alentar a registros y registradores a que actúen incluso cuando no hay una decisión judicial. Es decir, una notificación creíble debería ser suficiente para que registros y registradores actúen para que todos estemos seguros.

Quisiera también poner todo esto en contexto. Aquí en la siguiente diapositiva vamos a presentar a Alexander y vamos a tener un vínculo a su presentación. Quiero darles el título precisamente del convenio de Budapest. Sé que todos en Europa conocen lo que hace el Consejo de

Europa y Alexander nos va a dar una introducción bastante precisa también. No estoy muy segura de que esto sea conocido por todos nuestros colegas por fuera de Europa. Por eso espero que en esta oportunidad podamos difundir por qué la Convención de Budapest es el mayor logro que tenemos en la lucha contra la ciberdelincuencia.

Quisiera también llevar esta discusión a otras conversaciones que hemos tenido de geopolítica en la ICANN. En la siguiente diapositiva van a ver algo que hemos debatido aquí antes. Hemos tenido a los representantes de la ICANN que nos han dado actualizaciones sobre lo que sucede en la ONU. Pareciera que actualmente la ONU está muy fascinada y emocionada con el éxito que ha tenido el convenio de Budapest y por eso quieren tener el suyo propio. Esto no es algo que esté sucediendo ahora mismo ni que tampoco va a suceder mañana pero cuando tuvimos nuestras discusiones sobre geopolítica hablamos sobre cómo la comunidad puede evolucionar en estos procesos para representar mejor y proteger a los usuarios finales. De nuevo, esta es un debate de política sobre las tendencias en las que quizá nos queremos involucrar y tratar de averiguar si esto tiene sentido o no y de qué manera lo haríamos.

Por último les voy a mostrar un vínculo directo en estas discusiones y las conversaciones de geopolítica que hemos tenido. Aquí van a encontrar el documento en el sitio web de la organización de la ICANN y producido por organizaciones intergubernamentales junto con la ICANN donde se habla sobre los desarrollos actuales. Para hablar sobre este tema le voy a dar la palabra a Veni. Veni, sé que usted va a

presentar este documento mañana en una sesión más larga y más amplia. Por eso quiero alentar a todos los que están hoy en esta sesión a que escuchen y que participen también mañana en la discusión sobre las plataformas y las regulaciones. Hemos utilizado el documento de Veni, que es excelente y muy informativo, como un vínculo hacia los procesos internacionales y la protección del uso indebido del DNS.

Tengo una diapositiva más. Estas son las preguntas que vamos a tratar de responder durante esta sesión y le voy a pedir a Matthias que nos dé un ejemplo de cómo los usuarios finales pueden enfocar esto. Vamos a tratar entonces de ver si existe un vínculo entre el uso indebido del DNS y la ciberdelincuencia tal como lo vemos ahora en el plano internacional. ¿Existe un rol que la comunidad de la ICANN pueda tener en estas conversaciones internacionales? Finalmente, ¿ha fracasado el derecho? ¿Tenemos que reducirnos a políticas y normas que hemos desarrollado como la ICANN porque el derecho internacional tiene poco o nada para ofrecer? Sí, estoy tratando de ser polémica y ustedes saben que a mí me gusta hacer eso.

Con esto entonces me voy a detener. Le voy a dar la palabra a Matthias. Sé que Matthias también va a ser polémico. Eso es algo que yo recibo con agrado. Con esto le voy a dar la palabra. Me dijeron que tengo que ceñirme mucho al cronograma. Me extendí un poco más. Ahora le voy a dar la palabra directamente a Matthias. Luego le voy a pedir a Alexander que responda o que nos dé más detalles sobre

cuáles son las herramientas que podemos explorar. Ahora sí, le voy a dar la palabra a Matthias.

MATTHIAS HUDOBNIK: Hola a todos. Soy Matthias Hudobnik. Para quienes no me conocen, soy ingeniero y uno de los miembros del Comité Asesor At-Large. Como Joanna ya dijo voy a tratar de enfatizar los procesos legislativos actuales y su impacto en las políticas de uso indebido del DNS y qué es lo que se puede esperar. Las implicaciones están incluidas en un ejemplo práctico desde la perspectiva del usuario final. Mi charla va a ser breve y práctica para que tengamos suficiente tiempo para luego el debate. Después vamos a tener ese debate, no me cabe duda.

Este es Matt. Matt es un usuario final de Internet y, como pueden ver, tiene su propio dominio: www.matt.info. Perdió su dominio, por supuesto, pero un día ese dominio sufrió uso indebido. Matt está muy preocupado por este acto de delincuencia. ¿Qué creen ustedes que va a tener que hacer Matt como usuario final de Internet? En general, yo supongo que él se va a dirigir a la policía local y usualmente ellos van a actuar de conformidad con la ley de telecomunicaciones o penal aplicable que es más o menos lo mismo que ocurre en otro sistemas legales. Se toma en cuenta si es un sistema de derecho común, de derecho civil o mixto. Puede haber una relación que va más allá de las fronteras, transfronteriza, y que puede estar coordinada por la policía o por un esfuerzo de aplicación de la ley como en Europa la Agencia de Corporación de Aplicación de la Ley. Bajo ese mandato y el régimen de

la legislación europea, como dije antes, la investigación normalmente se basa en el derecho penal doméstico, local. Cuando un sospechoso reside en un país extranjero y se necesita asistencia legal, que se llama MLAT, se interroga al sospechoso en un caso penal. Siguiente diapositiva, por favor.

Vamos a ir un paso más. Como pueden ver aquí, en esta imagen muy polémica, esta imagen está censurada. Vamos a suponer que Matt tiene esta imagen en su sitio web porque es periodista y quiere atraer la atención a un evento. Se trata de un ejemplo en tiempo real. Esta imagen fue realizada el 8 de junio de 1972 y es una foto de las fuerzas de Vietnam del sur que están persiguiendo a niños que están aterrorizados. Esta imagen ganó el premio Pulitzer. También dio lugar a mucho debate en Noruega sobre la libertad de expresión. Facebook dijo que esa fotografía se trata de pornografía infantil y la eliminó porque eso violaba sus estándares sobre la desnudez. Se trata de humanos, no de algoritmos, quienes desde Facebook decidieron eliminar esta publicación. La imagen censurada también violaría las normas de ICANN y esto se refiere a la introducción de Joanna. Siguiente diapositiva.

Como Joanna ya nos dijo, estamos aquí hablando de distintos marcos, distintos marcos legales, distintos niveles y en particular quiero referirme al marco del DNS que está firmado por 48 registros y registradores que están regidos por estos principios y el punto en particular que quiero poner de relieve aquí es cuándo un registro o registrador debe actuar en relación con el uso indebido del contenido

de un sitio web. Especialmente quiero enfatizar el hecho de que en este documento se establece que el registro o registradores debe hacerlo sin una orden judicial. No voy a repetir aquí lo que está escrito pero lo que me sorprende en particular es esta redacción. De todos modos me voy a referir a esto más adelante. También podemos ver una escala. También procede del documento. Muestra los lugares en los que se puede remover el contenido antes de escalar al revendedor y luego aparecen el registrador y el registro. El documento también establece que un registrador o un registro pueden darlo de bajo y quien presenta la queja puede tener daños potenciales.

Estos son puntos muy interesantes y no quiero entrar en una discusión de contenido porque va a haber una sesión adicional. Esto queda por fuera del alcance de esta sesión. De todos modos, quiero hablar sobre la definición que escribí yo en esta diapositiva. ¿Qué puede significar esto para el usuario final y cómo afecta esto al usuario final? Traté de generar una imagen y que esto sea práctico desde la perspectiva del usuario final. Uno puede decir: “Está todo bien. Puedo dirigirme a mi registrador o mi registro, que van a actuar en mi beneficio sin una orden judicial. Van a hacer lo que está indicado en este documento”.

Por otro lado también se puede decir: ¿Por qué tenemos todos estos marcos legales y regulaciones donde están incluidas también las personas que deciden y quienes toman las decisiones educativas? Lo hacen en forma independiente y de una forma más o menos efectiva. Por supuesto, esto se puede debatir.

No me malentiendan. Yo no estoy aquí para resolver este problema. Tampoco estoy aquí para decir que no tenemos que pensar en soluciones adicionales para resolver estos usos indebidos. Creo que es crucial hablar de este tema y quiero señalar las ventajas y desventajas potenciales dependiendo por supuesto del punto del que venimos. Como pueden ver aquí en esta diapositiva, la pregunta que realmente llamó mi atención es cómo podemos garantizar los derechos fundamentales como la libertad de expresión, si estamos de acuerdo con estas soluciones de DNS. Cómo podemos solucionar el problema del uso indebido del DNS para los usuarios finales de manera realista teniendo igual protecciones implementadas para evitar el uso indebido o la censura. ¿Quién debería ocuparse de la revisión? ¿Quién debería tomar la decisión? Además, ¿quién debe decidir concretamente a nivel de registro y registrador y en qué función, en qué rol?

Finalmente, cómo obtendrán los decisores las habilidades necesarias respectivas si es que acordamos que estas son las soluciones para el DNS. Habiendo dicho esto termino mi presentación. Les agradezco por haberme dado la oportunidad de hablar con ustedes. Le doy la palabra al siguiente orador.

JOANNA KULESZA: Muchas gracias, Matthias. Le doy la palabra a Alexander.

ALEXANDER SEGER: Muchas gracias. Espero más allá de esta sesión de una hora poder seguir dialogando con ustedes. El título sin duda era polémico y yo dije que no es una cuestión de ir más allá de Budapest sino de ir junto con Budapest. Cooperación global sobre ciberdelito incluido el uso indebido del DNS. El convenio de Budapest sobre ciberdelincuencia comenzó en Budapest en 2001. Si consideramos la ciberdelincuencia y el Convenio de Budapest vemos que es un marco global para la cooperación sobre la ciberdelincuencia. El ciberdelito, incluido el uso indebido del DNS, es una cuestión de justicia penal. Los gobiernos tienen la obligación de proteger. Es decir, no solamente tienen que protegernos de que no se violen los derechos sino también protegernos contra el delito. Hay decisiones muy importantes relacionadas con el Convenio de Budapest que se tomaron en 2008 en una sentencia del Reino Unido vs Finlandia, una sentencia muy importante.

El ciberdelito y las cuestiones de evidencia electrónica requieren una respuesta efectiva en términos de la justicia penal y esto es lo que nos da el Convenio de Budapest. No es un instrumento de seguridad nacional ni tampoco de inteligencia. Se trata de especificar los datos que se necesitan en determinadas investigaciones penales. Tal como dijo Matthias cuando habló de los derechos de las personas y la forma de protegerlos y de proteger estos derechos, debemos recordar que la respuesta de la justicia penal también es proteger. Sí, hay facultades para procesar y juzgar pero estas facultades están limitadas por el estado de derecho y por las protecciones que apuntan a proteger los

derechos de las personas incluidas las personas sospechosas y para evitar también el abuso y el uso indebido. Esto es muy importante.

También debemos recordar que la respuesta de la justicia penal complementa otras medidas que apuntan a evitar las amenazas pero es difícil evitar y responder a las amenazas de seguridad. La respuesta de la justicia penal es un elemento importante de una respuesta mucho más amplia. En esta diapositiva vemos que, tal como subrayó Matthias también, tenemos que ser muy cuidadosos y no violar libertades en Internet.

Si vemos el Convenio de Budapest, la presunción inicial es el libre flujo de la información y el acceso a la información. Debe ser posible compartir información pero también existe la obligación de proteger contra las restricciones de flujo de cierta información en Internet. Es muy importante esto. Este es el fundamento del Convenio de Budapest. La idea es ampliar el alcance geográfico del Convenio de Budapest, extenderlo a todo el mundo. Eso es por un lado lo que ocurre con respecto al Convenio de Budapest.

Por otra parte tenemos algunas contrapropuestas. No digo que esto sea específicamente lo que indica el tratado de Naciones Unidas sobre delitos. Esta es una propuesta de un tratado que abarca estas ideas. El foco está en los delitos de información. No ciberdelitos sino delitos relacionados con la información basados en la doctrina de la seguridad de la información. La idea subyacente es que los gobiernos tienen el control soberano de su espacio de información. En este

sentido, los gobiernos también controlan a qué información deberían estar expuestas las personas. Hay algunos conceptos de delito que están definidos de una manera un poco vaga. Hay protecciones restringidas y, como probablemente no se alcance un consenso con respecto a estos temas, el riesgo es que el resultado genere una fragmentación adicional y se creen esferas de influencia en lugar de una respuesta general. Ese es el riesgo que vemos y que escuchamos entre las partes del Convenio de Budapest. Pasemos a la siguiente diapositiva, por favor.

¿De qué se trata el Convenio de Budapest? Es un convenio que indica que las partes tienen que hacer tres cosas. Tienen que acordar que van a actuar contra delitos específicos por medios de sistemas informáticos. Tienen que tener facultades procesales para investigar los ciberdelitos y recopilar evidencias electrónicas en relación con todos los delitos y también tienen que participar en la cooperación internacional sobre ciberdelito y sobre cualquier delito que involucre evidencias electrónicas. Este tratado tiene 20 años de antigüedad pero se ha complementado con diferentes documentos guía. Hay algunas notas adoptadas por las partes del convenio que dicen que esta es la forma en la que aplicamos las cláusulas del convenio a fenómenos más recientes. Actualmente hay diferentes negociaciones sobre los delitos informáticos.

El Convenio de Budapest es un marco que vemos aquí en este triángulo. Tenemos el Convenio de Budapest y los estándares relacionados, estándares de protección de datos, de protección de

derechos, protección de niños, etc. Luego tenemos también el Comité para la Convención sobre el Ciberdelito. Son las partes de este tratado incluyendo al secretario del comité. Luego hacemos creación de capacidades a través de la oficina del programa global de ciberdelito que tiene las facultades para actuar. El convenio incluye todo esto. Es un mecanismo, no solamente un tratado. Ahora ya hay 65 partes y 12 estados adicionales que decidieron firmar y adherirse al Convenio de Budapest. La siguiente diapositiva, por favor.

Si lo miramos desde el punto de vista del ciberdelito relacionado con COVID, phishing, malware, ransomware, botnets, DDoS, spam, fraude, encontramos todos estos fenómenos encubiertos aquí. Es decir, se criminalizan muchas de estas herramientas pero hay una guía que muestra cómo se pueden utilizar diferentes cláusulas para afectar sobre malware, spam, etc. En cierta forma todo esto está cubierto en un documento. Las partes que implementan el Convenio de Budapest tienen los medios para actuar contra este tipo de ciberdelitos relacionados con la COVID. Además, tienen las facultades procesales para investigar, obtener evidencias y luego juzgar y condenar a quienes cometen los delitos con ciertas protecciones. También hay notas de guía que explican un poco mejor cómo se pueden utilizar las facultades procesales. Finalmente tenemos el marco de cooperación internacional, porque también se puede cooperar a nivel internacional contra este tipo de delitos. El marco existe. No podemos decir que no tenemos suficiente información. Con el Convenio de Budapest este

tipo de delitos se penaliza. La idea es cooperar y penalizar este tipo de delitos.

Como dije, actualmente tenemos más de 60 partes. Las más recientes fueron Perú y Colombia. Hay muchos otros países que fueron invitados. Nueva Zelanda también fue invitada. Nueva Zelanda está finalizando con su proceso local. Hay países no solamente de Europa sino también de Asia. Tenemos Filipinas, Japón, Sri Lanka en África. Tenemos Ghana, Senegal, las Islas Mauricio, Cabo Verde y otras partes. Tenemos también Canadá, Costa Rica, Argentina y muchos otros países. No se trata de un instrumento europeo solamente sino más bien un instrumento global pero además de estos 77 estados de partes o de países que pronto van a ser partes, hay muchos otros, casi el doble, que utilizan el Convenio de Budapest. 108 estados en todo el mundo han actuado a nivel penal en sus propios países basándose en el Convenio de Budapest. Esto es algo que es muy importante y que debemos entender. La próxima diapositiva, por favor.

Hay un nuevo protocolo que está en curso. Comenzó en septiembre de 2017. Esperamos que pronto finalicen las conciliaciones. Hay otras cosas que hay que hacer. Luego esperamos poder abrir este protocolo para que sea firmado en el año 2021, el próximo año.

¿Por qué se necesita este protocolo? Es muy importante por este problema de la territorialidad y la jurisdicción. Tal como dijo Matthias, las facultades de las autoridades de aplicación de la ley se ven limitadas a la jurisdicción, a sus propios territorios. Si queremos

evidencias de algún otro lugar, de algún otro país, en general tenemos que obtenerlas a través de asistencia mutua. Si uno no sabe muy bien cómo obtenerla es muy difícil avanzar. Se trata de un problema muy complejo de jurisdicción, territorialidad. Es por eso que se tomó la decisión. A veces la eficiencia de la asistencia mutua no es muy grande. Se decidió que era necesario contar con un nuevo protocolo que comenzó hace tres años. La próxima diapositiva, por favor. A continuación vemos la siguiente diapositiva. Muchas gracias.

Muy brevemente, cuáles son los elementos del protocolo. No puedo entrar en detalle porque me llevaría demasiado tiempo pero en este protocolo se incluirán cláusulas para asistencia legal mutua más eficiente. Cómo podemos hacer que todo este proceso para obtener datos a través de las relaciones gubernamentales sea más eficaz, más eficiente, más oportuno para poder también obtener evidencias y continuar con los procesos tradicionales. Es muy importante el hecho de que probablemente haya dos cláusulas sobre la cooperación acelerada. Una es a través de la asistencia mutua, asistencia mutua de emergencia de forma tal que incluso en un fin de semana, cuando los ministerios de justicia están cerrados, igual podamos obtener asistencia mutua a través de las partes de este protocolo.

Hay otra cláusula más mediante la cual los países pueden recurrir a procedimientos locales para acceder a contenido, información sobre contenido y sobre tráfico en una emergencia si se trata de vida o muerte. Estas son cláusulas muy importantes para la cooperación en situaciones de emergencia.

Luego hay otro punto interesante que es esta idea de que las autoridades de un estado, de un país pueden cooperar directamente con un proveedor de servicio que está en otra jurisdicción, en otra parte. Hoy estoy en Rumanía, Bucarest. Rumanía necesita datos de las Islas Mauricio. Pueden cooperar directamente con el proveedor de servicios de Mauricio, Estados Unidos, o donde fuera. Hace un tiempo publicamos una versión preliminar de este documento. Uno puede acceder a información de otra parte directamente. Con ciertas protecciones que son claras es posible acceder a esta información.

Luego hay un punto muy interesante probablemente para la comunidad de la ICANN. Estamos considerando si podemos crear una base legal para solicitar la divulgación de información de WHOIS por parte de los registros y los registradores. Este es un tema que se está negociando en este momento. Esperamos pronto contar con una versión preliminar y esperamos ver también el aporte de otras partes interesadas. La idea no es sustituir WHOIS en el contexto de la ICANN sino complementarlo, contar con las bases legales para todo tipo de mecanismos, procedimientos, reglamentaciones que surjan a través del proceso de la ICANN. Si pasamos a la cooperación acelerada y cooperación en caso de emergencia, podremos cooperar directamente con proveedores de servicio, con divulgación de información de datos de WHOIS. Si esto ocurre, entonces deberemos contar con fuertes protecciones de datos incluidas en este protocolo, con GDPR, con los sistemas legales de todos los países que sean parte de estos protocolos. Este es un debate sumamente complejo. Yo creo que en los

próximos meses vamos a contar con toda la información disponible y esperemos que el protocolo esté disponible para la firma del próximo año. La última diapositiva, por favor.

Las conclusiones. Lo que ocurre en otros foros, Naciones Unidas o en otras partes es importante en relación con el convenio de Budapest. Este protocolo probablemente sea el instrumento más pertinente, más relevante para la justicia penal en relación con los ciberdelitos. Las partes tienen que participar en este proceso. Las cláusulas de cooperación internacional del convenio están disponibles para investigar y juzgar el uso indebido del DNS. Hay debates en curso incluyendo los debates sobre la base legal para solicitudes de divulgación de información de registración de nombres de dominio entre todas las partes que forman parte de este protocolo. Esperamos que el protocolo esté finalizado pronto y que contemos con una versión preliminar para iniciar un debate público y recibir los comentarios de todas las partes interesadas. Muchas gracias.

JOANNA KULESZA: Muchas gracias. Esto ha sido muy informativo. Veo que hay muchas preguntas que aparecen en el chat. He tomado nota de algunas de las preguntas. Algunas son sobre las actividades de generación de capacidad. Quisiéramos escuchar un poco más. Algunas de ellas son de aspectos específicos o de la implementación de la convención. Sé que hay respuestas. Lo que quisiera hacer es darle la palabra a la primera mano levantada que tenemos, que viene de Hadia. Si Hadia

puede hablar, le voy a dar entonces la palabra para escuchar su retroalimentación, la retroalimentación de los participantes. También vamos a mirar las preguntas. Le voy a preguntar a Alex si quiere contestar una por una o todas juntas. Luego los aliento a que levanten la mano, como hizo Hadia, y que tomen la palabra para interactuar con nuestros oradores. Hadia, tiene la palabra ahora.

HADIA ELMINIAWI: Gracias, Joanna. Mi pregunta tiene que ver con lo que se acaba de presentar. La convención es un tratado internacional que es obligatorio en lo que se refiere a la ciberdelincuencia. Tiene el objetivo de proteger a la sociedad a través de legislación adecuada contra el ciberdelito pero también apuesta por la cooperación internacional. Mi pregunta entonces es sobre las partes de la cooperación internacional. En lo que se refiere al ciberdelito o al uso indebido del DNS, como definitivamente podemos ver, todo esto está cubierto y está criminalizado incluso por el convenio. ¿Puede la ICANN efectivamente actuar como un régimen para que esta cooperación internacional ocurra? Eso es solo una parte. De nuevo, es obvio que de lo que estamos hablando en cuanto al abuso del DNS está criminalizado pero el problema son las medidas que se deben tomar. En relación con ICANN, la pregunta es si puede haber un régimen a través del cual esa cooperación pueda ocurrir, especialmente si tenemos en cuenta asuntos como el WHOIS o los datos de registración. La comunidad de hecho ya está trabajando sobre estos asuntos. Gracias.

JOANNA KULESZA: Gracias, Hadia. Quizá, Alex, te pueda resultar útil que me refiera al proceso de desarrollo de políticas que se focaliza en llamémoslo WHOIS, pero no es tanto WHOIS como un marco de implementación. Hadia ha sido muy activa en tratar de mantener a la ICANN a la altura de estos procesos internacionales. Si es posible, quisiera que se refiera a estas preguntas específicas y luego pasamos a la larga lista que tengo aquí que hace referencia a los distintos aspectos que el consejo de Europa está haciendo. Quiero recordarles el tiempo y por eso me disculpo por adelantado si me salteo alguna pregunta. Alex ya indicó que él nos puede responder después porque va a haber un canal de comunicación que podemos abrir para esta colaboración para que persista. Alex, si quiere responder primero a la pregunta de Hadia, sería excelente. Gracias.

ALEXANDER SEGER: Las organizaciones como la ICANN y los registros y registradores, proveedores de registros en el amplio sentido de la palabra, incluso otras autoridades de aplicación de la ley, cuando hablamos de la acción y la toma de decisiones son las autoridades las que deben decidir. El EPDP, el WHOIS, etc. son un buen ejemplo de que va a haber un mecanismo efectivo que va a surgir a partir del proceso a través de la divulgación de la información del WHOIS pero de todos modos las autoridades deben tener una base legal clara para poder actuar. Eso es lo que estamos tratando de lograr a través del Convenio de Budapest.

De nuevo, es un esfuerzo cooperativo pero creo fuertemente que las acciones de la justicia penal deben quedar en ese marco.

JOANNA KULESZA: Gracias por aclarar, Alex. Matthew, te voy a dar la palabra pero vamos a mirar las preguntas. Las vamos a ver en orden cronológico. La primera es de Judith Hellerstein. Gracias, Judith, por hacer esta pregunta. Sé que a Alex le va a interesar. Usted nos dio un resumen del trabajo que se está haciendo dentro de At-Large. Tenemos una comunidad de AFRALO que es muy activa en lo que se refiere a la generación de capacidad. Si hay algún miembro de AFRALO aquí, en esta reunión, estoy segura de que ellos van a agradecer un feedback sucinto pero informativo en términos de generación de capacidad, ciberdelitos, el Convenio de Budapest. Yo diría también un efecto que nos permita continuar en países que no son signatarios. ¿Sería esto posible, Alex?

ALEXANDER SEGER: Sí. En 2013 se decidió establecer específicamente una oficina del programa de ciberdelito que se respalde a países en cualquier lugar del mundo para fortalecer la legislación y otros dominios. Hay una oficina que está en Bucarest, en Rumanía. Se estableció en 2013. Entró en operación en 2014. Tenemos varios programas para África, Asia, América Latina, el Pacífico, etc. Se ha extendido ahora a una segunda fase sobre el ciberdelito. Es un proyecto conjunto de la Unión Europea y del Consejo de Europa. Hay un presupuesto bastante importante de

19 millones de euros que se está considerando ampliar. Se puede dar apoyo a cualquier país. Hay tanta demanda que se focaliza en países que se han comprometido a unirse al convenio de Budapest. Hay todo un menú de actividades, capacitación, etc. en Nigeria, en Ghana, en Senegal, en Mauricio, etc. De todos modos, podemos dar apoyo a otros países para fortalecer la legislación local. Hay muchas otras actividades también en Namibia, por ejemplo, en Congo. También ellos están trabajando. En Fiji y en otros. Para el menú total necesitamos que haya un compromiso de firmar el Convenio de Budapest. Por eso estamos trabajando con 40 países ahora.

JOANNA KULESZA: Gracias. Muy informativo. Sé que el consejo de Europa tiene una oficina y un personal muy eficiente y que les pueden dar más información. Tenemos dos preguntas de Stephanie Perrin de nuevo, que es una miembro muy activa y se focaliza en la priorización de la privacidad y la seguridad. Stephanie nos pregunta: “Con respecto a las protecciones, ¿por qué no insistir en que aquellos que quieren firmar el Convenio de Budapest también deben ser signatarios de la Convención 108?” Creo que podemos vincular esto a la segunda pregunta. “En cuanto a la jurisdicción, ¿va a haber un control de protección de datos tal como existe en una oficina en Europa en Eurojust? ¿Hay problemas similares con respecto a las necesidades de soluciones de control de protección de datos?”

Me da curiosidad saber si quizá usted nos puede contar algo sobre los defensores de la privacidad dentro de la comunidad de la ICANN que siempre están preocupaciones por la necesidad de priorizar seguridad y privacidad. Entiendo que de ahí provienen las preguntas de Stephanie. Sería excelente si pudiésemos tener su feedback sobre la ciberdelincuencia en relación con la privacidad.

ALEXANDER SEGER: Voy a responder pero voy a hacer otro recordatorio. Creo que fue en la segunda o tercera diapositiva que yo dije que el derecho penal está protegido. Tenemos un derecho procesal penal para poder regular de qué manera los gobiernos o las autoridades pueden interferir en los derechos. El derecho penal está protegido. Debe quedar muy claro esto. Hay muchas salvaguardas, muchas protecciones, más allá de la protección de datos para el derecho penal. Es decir, esto es menos frecuente en mi opinión en cuanto a la seguridad nacional. Después de algunos escándalos, de algunas revelaciones, quedó en claro qué es lo que hacen algunas instituciones nacionales. El derecho penal tiene menos protección. Es una dinámica muy extraña.

En cuanto a la Convención 108, o 108+ como se le llama ahora en la forma más moderna, no es una coincidencia que muchas de las partes no europeas como Mauricio, Senegal, Argentina y otros son también partes signatarias de la Convención 108. Es muy importante. Actualmente le estamos dando apoyo por ejemplo a Namibia en la reforma de su legislación sobre ciberdelincuencia pero también

estamos dando apoyo al informe de la legislación sobre protección de datos. Lo mismo en Sri Lanka. Estamos trabajando con otros países como la República Dominicana. Estamos muy a favor de esto.

En el Convenio de Budapest es muy difícil de negociar. Hay que tratar de tomar estas normas y proceder con el protocolo en sí. No hacer una referencia cruzada a otras normas sino tomar el Convenio de Budapest en forma global. Una de las subdisposiciones va a ser sobre las autoridades supervisadas. Por lo tanto, también va a tener que haber funcionarios de protección para que las normas sean respetadas. Si una de las partes transfiere datos a otra parte, esa parte puede estar segura de que los datos van a estar protegidos y que va a haber una norma similar en la parte que recibe.

JOANNA KULESZA: Gracias, Alex. Vamos a pasar rápidamente. Tenemos 12 minutos. Tenemos algunas preguntas más generales. Una de Olevie Kouami que pregunta: "¿Cuál es el estado de la relación entre la Convenio de Budapest y la de Malabo?" Quizá usted nos pueda responder. Supongo que esto se refiere a Alex también.

ALEXANDER SEGER: La Convención de Malabo de la Unión Africana de alguna manera fue más breve. La Convención de Malabo se refiere a la protección de datos. También a la ciberseguridad, etc. Lo que tenemos que ver es cuál es la relación entre el lado del ciberdelito de una convención y de

otra. Aquí hemos discutido y analizado en detalle en las distintas discusiones que tuvimos con la Unión Africana, vemos esto como una complementariedad perfecta porque la Convención de Malabo está limitada y no nos ayuda a cooperar con Estados Unidos. Solamente ocurre dentro de África y no contiene difusiones específicas sobre cooperación internacional sino que se refiere a un sólido compromiso porque ha sido adoptado por los jefes de estado y de gobierno de varios estados. Tenemos un acuerdo con la Unión Africana de que en conjunto podemos promover la implementación de la Convención de Malabo y la de Budapest al mismo tiempo.

JOANNA KULESZA: Muchas gracias, Alex. Tengo otra pregunta más general de Siva. "¿Podría haber un proceso de cambio de respuesta interjurisdiccional?" Alex, ¿escuchó la pregunta?

ALEXANDER SEGER: Sí, pero no sé a qué se refiere.

JOANNA KULESZA: ¿Podemos hacer cumplir la ley rápidamente? Entiendo que eso es lo que preguntan. ¿Podríamos hacerlo rápidamente y de manera eficiente?

ALEXANDER SEGER: Actualmente, en el Convenio de Budapest hay una serie de indicadores y de medidas que permiten acción inmediata. Por ejemplo, si se necesita un llamado telefónico, un correo electrónico, eso se puede obtener en cuestión de horas. Hay varias cláusulas del convenio actual de Budapest que incluyen esto. También el acceso a puntos de contacto. En el protocolo futuro habrá algunas cláusulas que irán más allá de esto. Es decir, se podrá llamar directamente a un proveedor de servicios en otra parte, en otro país y obtener información. Una vez más, considerando que habrá ciertas protecciones.

Además, hay una serie de cláusulas que estarán incluidas en el protocolo que permitirán una ejecución más eficaz para quizá un proceso de MLA, de asistencia legal mutua tal como dijimos que permitan avanzar más rápidamente. En caso de una emergencia, ya sea un ataque terrorista en curso y necesitamos acceso a los datos en otro país, tenemos que poder acceder inmediatamente como lo que ocurrió en Nueva Zelanda, en París, Charlie Hebdo, etc. Incluimos dos cláusulas que permiten acceder muy rápidamente a estos datos en situaciones de emergencia. Sí, habrá formas de llevar a cabo medidas penales y legales de manera mucho más rápida. Ya existe actualmente en el convenio pero en el futuro también estará incluido.

JOANNA KULESZA: Gracias, Alex. Hay otra pregunta abierta entiendo yo. Gracias por plantear esa pregunta. ¿Las partes necesitan firmar todos los protocolos adicionales al firmar también este protocolo?

ALEXANDER SEGER: Uno no puede adherirse a un protocolo si no se adhiere primerio al convenio pero sí se puede unir al convenio sin adherirse a los otros protocolos. Le voy a dar un ejemplo. Este es el primer protocolo por el momento. Ahora estamos trabajando en el segundo protocolo. El primer protocolo de 2003 era sobre xenofobia y actividades a través de sistemas informáticos. Era muy importante para países africanos y europeos. Se llevaron a cabo varias negociaciones. En algunos países, Estados Unidos es uno de estos países, la libertad de expresión está tan protegida que ellos dijeron que no podían unirse a este protocolo. Creo que el protocolo está firmado por 35 o 36 partes. El convenio tiene 65. Hay 30 partes que están en el Convenio de Budapest y que no son parte del primer protocolo.

Con respecto a este segundo protocolo, el protocolo futuro, incluimos algunas cosas que son muy atractivas y que todos necesitamos. La base legal para acceder a datos de WHOIS, la posibilidad de cooperar directamente. Esto es muy importante. También este segundo protocolo será más atractivo para que otros países también se unan al convenio. Primero deben formar parte del convenio e inmediatamente después pueden adherirse al segundo protocolo. No necesitan adherirse al primer protocolo.

JOANNA KULESZA: Muchas gracias. Creo que esto es muy claro y es algo que también surgió en los comentarios de Michael Graham, que enfatizó el hecho de

que en el caso del uso indebido del DNS deberíamos incluir también otros derechos como derecho de privacidad o violaciones de la libertad de expresión, discurso del odio que siempre es difícil. Para no entrar en detalle, porque estoy mirando el reloj, nos quedan cinco minutos. Tengo cuatro preguntas más. Con permiso de los miembros del panel voy a plantear estos temas y luego les voy a pedir que hagan algunos comentarios de cierre. Me dijeron que si me paso de mi tiempo todos los participantes van a ser condenados a muerte y no quiero correr el riesgo. Voy a plantear las preguntas y luego le voy a pedir a los panelistas que por favor resuman brevemente sus comentarios. Le agradezco mucho por su predisposición a interactuar con nosotros. Muchas gracias, Alex.

Voy a plantear las preguntas y después espero poder reservarles unos minutos para sus comentarios. Una pregunta de Elizabeth. "¿Cuál es la base legal para acceder a la información de registración de nombres de dominio? Usted se refirió a las partes. Cuando habla de las partes, ¿quiénes son las partes? Entidades gubernamentales, no gubernamentales".

Hay otra pregunta de Siva. Las mentes creativas judiciales o el estado de derecho deberían poder crear propuestas interesantes. ¿Por qué hablar de esto antes de incluso generar ciertas ideas para avanzar en este sentido? Es una invitación para seguir trabajando de manera creativa.

Hay una pregunta de Rick. La Comisión Federal de Comercio de Estados Unidos vio un aumento en el fraude online en torno a la pandemia de COVID-19. ¿La falta de acceso a los datos de WHOIS debido a GDPR ¿obstaculizó el trabajo de las autoridades de aplicación de la ley?

Luego hay una pregunta de Zakir. “Gracias por este debate tan útil. Esta es una pregunta para Alex. Dado que hay un debate sobre el tratado de Naciones Unidas sobre delincuencia propuesto por Rusia, seguramente Alex podrá hablar acerca del contenido de ese tratado propuesto por Rusia que ya logró bastante apoyo. ¿Piensa usted que tanto la Unión Europea como el tratado sobre ciberdelincuencia y el convenio podrán coexistir o existir en paralelo?” Yo creo que soy culpable por la confusión. ¿Por qué tenemos un tratado de ciberdelito de Naciones Unidas? Hemos hablado aquí sobre este tema en la ICANN. También hay un debate sobre ciberdelito que se acaba de iniciar.

Finalmente, con respecto al último punto de su última diapositiva, ha hablado acerca de la base legal para solicitar acceso a datos de WHOIS. Alex, usted mencionó consultar con diferentes partes interesadas dentro de la ICANN para recopilar, confrontar o acceder a esta información. En ese caso, ¿en qué marco, en qué momento? Estas son las preguntas. Nos quedan solo dos minutos. Le voy a dar un minuto a Alex para que nos dé un comentario emocional. Esperamos que se hayan sentido bienvenidos. Las preguntas demuestran mucho

interés. Quisiera que nos dé un breve resumen y luego le voy dar la palabra a Matthias para que nos dé su comentario de cierre también.

ALEXANDER SEGER: La primera pregunta era acerca del protocolo futuro, base legal, acceso a WHOIS y quién puede acceder. El convenio de Budapest es un tratado de justicia penal. Tenemos que remitirnos a nuestras competencias. No podemos excedernos. La base legal para la justicia legal tiene ciertos límites en cuanto a acceder a los datos. Creatividad. Sí, necesitamos creatividad. Creo que la justicia penal es muy conservadora. Es muy difícil cambiar las cosas. Seguimos trabajando en temas de jurisdicción que fueron definidos hace unos 100 años cuando se definió la jurisdicción en el nivel internacional. Tenemos que trabajar de manera creativa y tenemos que avanzar con este protocolo para poder seguir avanzando.

A partir de lo que entiendo en función de la aplicación de la ley, sí, hay ciberdelitos relacionados con COVID. Hemos visto un gran pico. Parte del problema podría deberse al acceso limitado a datos de WHOIS. El tratado de ciberdelincuencia de Naciones Unidas podría llamarse tratado de ciberdelincuencia. Quizá debería ser un tratado de seguridad de la información. Hay otros tratados de Naciones Unidas, del Consejo de Europa sobre corrupción y muchas otras áreas, lavado de dinero. Por supuesto, todos estos tratados pueden coexistir pero no sabemos todavía cuál será el contenido del tratado de Naciones Unidas para los delitos cometidos a través de las tecnologías de la

información y la comunicación. Creo que esos son los términos que se están utilizando en este momento.

Con respecto a la consulta sobre el protocolo del año pasado a fines de noviembre tuvimos la primera ronda de consultas. En ese momento no era sobre WHOIS sino sobre otros elementos. Había representantes de la ICANN. Había 450-460 personas involucradas. Tenemos que hablar acerca con las diferentes partes. Es probable que una vez que tengamos la propuesta de WHOIS invitemos a los gobiernos pero al principio del próximo año, cuando ya contemos con la versión preliminar del protocolo, probablemente llevemos a cabo consultas con las partes interesadas y esperamos que la comunidad de la ICANN, que todos ustedes participen en esta consulta. Podrán enviar comentarios por escrito y esperamos también poder organizar por lo menos una reunión virtual para que todos podamos hablar acerca de los comentarios recibidos y para que podamos ver también cómo podemos tomar en cuenta estos comentarios y finalizar el protocolo incluyéndolos.

JOANNA KULESZA: Muchas gracias, Alex. Les pido disculpas. Debería haber dejado más tiempo para la conversación. Le prometí unos minutos a Matthias. Matthias, ¿podría resumir este increíble intercambio en el último minuto que nos queda?

MATTHIAS HUDOBNIK: Quiero agradecerles a todos por este debate tan interesante. Espero que podamos luego ver las preguntas después de la presentación. Es probable que surjan nuevas protecciones en relación con el uso indebido del sistema de nombres de dominio y los usuarios finales. Tal como ya dije, tenemos diferentes marcos y esto tiene que ver con el trabajo en el área penal y se están llevando a cabo proyectos para encontrar soluciones. Se están coordinando estas diferentes actividades en los países en los que se produce el uso indebido. Quizá necesitemos encontrar soluciones adicionales. Ahora tenemos muchos casos relacionados con COVID y es importante que encontremos formas de involucrar a las partes interesadas para que podamos encontrar todos una solución. Gracias.

JOANNA KULESZA: Muchas gracias. Creo que este es un mensaje final excelente. Muchas gracias, Alex, por haber participado hoy. Sé que tiene una agenda sumamente ocupada. Gracias por haberle explicado a esta comunidad cómo funciona el trabajo que están haciendo ustedes en el Consejo de Europa y cómo podemos proteger a los usuarios finales. Voy a terminar aquí la sesión sin hacer un resumen final. Muchas gracias a los panelistas. Excelente. Gracias a todos por haber estado aquí con nosotros, por el activo debate en el chat. Trataremos de continuar con este debate en el contexto del uso indebido del DNS y el contexto del Convenio de Budapest. No tenemos que ir más allá de Budapest, tal como dijo Alex claramente. Muchas gracias al personal. Gracias al equipo técnico. Les pido disculpas a los intérpretes por haber tomado

demasiado tiempo. Aquí voy a dar por cerrada la sesión. Gracias a todos por participar.

[FIN DE LA TRANSCRIPCIÓN]