DUBLÍN – Sesión abierta del Grupo de trabajo del GAC sobre seguridad pública
Lunes, 19 de octubre de 2015 – 15:00 a 16:30 IST
ICANN54 | Dublín, Irlanda

ALICE MUNYUA: En esta sesión vamos a hablar del tema de la seguridad pública así que me parece que por el tipo de tema que vamos a tratar, sería mejor si pudieran acercarse al frente, a las primeras filas, y no estén tan lejos.

Buenas tardes a todos. Es una sala tan grande que les pedimos por favor que se acerquen un poco para que esta sea una reunión un poco más íntima. Sabemos que estamos compitiendo con otras sesiones, la del CCWG… pero esta es muy importante así que nos gustaría que se sentaran más cerca de nosotros. Gracias.

Buenas tardes. Soy Alice Munyua. Esta es una reunión del Comité Asesor Gubernamental, específicamente del grupo de trabajo sobre seguridad pública de este comité. Es un grupo de trabajo que fue establecido según el principio 27 del GAC y se focaliza en los aspectos de las políticas y procedimientos de la ICANN que tienen implicancias para la política pública. Fue creado oficialmente en Buenos Aires. Los términos de referencia fueron oficialmente avalados por el GAC y los principales miembros son representantes de organismos de aplicación de la

ley, países y distintos grupos de defensa de consumidores, de protección de los consumidores, grupos de aplicación de las leyes y que combaten el delito y otros organismos responsables de la seguridad pública.

Si les interesa tener un detalle mayor de los términos de referencia de este grupo de trabajo del GAC pueden ingresar al sitio web del GAC donde hay un espacio de trabajo donde están esos términos. Tenemos un temario bastante extenso pero vamos a presentar a los panelistas. Yo soy copresidente de este grupo de trabajo en representación de la Comisión de la Unión Africana. Mi nombre es Alice Munyua.

WANAWIT AHKUPUTRA: Wanawit Ahkuputra de Tailandia. También soy vicepresidente del GAC.

LAUREEN KAPIN: Soy Laureen Kapin de Estados Unidos, de la Comisión Federal de Comercio focalizada en la protección de los consumidores.

ROBERT FLAIM: Bobby Flaim del FBI.

JOHN CARR: John Carr, represento a la Coalición de las Entidades de Beneficencia Británica para los Niños sobre la seguridad infantil en Internet.

CATHERIN BAUER-BULST: Catherin Bauer de la Comisión Europea y líder del equipo que lidera la lucha contra el ciberdelito y el abuso sexual.

GREGORY MOUNIER: Yo soy Gregory de la Europol, agencia de aplicación de la ley europea, ocupándonos del centro de ciberdelitos europeos.

NICK SHOREY: Yo soy miembro del Ministerio de Cultura, Medios y Deportes en Reino Unido.

JON FLAHERTY: Soy John Flaherty. Yo pertenezco a la Unidad Nacional de Ciberdelitos.

ALICE MUNYUA: Muchísimas gracias. Tenemos panelistas sumamente distinguidos y esperamos tener muy buen debate aquí. Vamos a comenzar. Tenemos un temario bastante completo. En primer lugar vamos a tener un informe actualizado sobre lo que el

grupo de trabajo de seguridad pública ha estado realizando desde la reunión de Buenos Aires. Luego vamos a hablar del WHOIS y de las leyes de protección de los datos de Europa. Vamos a tener también ejemplos de WHOIS de Europol y vamos a ver una hoja de ruta sobre la labor que hará el grupo de trabajo de seguridad pública a nivel nacional y en coordinación con el nivel nacional. Luego la especificación 11 del marco de seguridad de los nuevos gTLD y una presentación sobre la explotación infantil y las cadenas de gTLD nuevas.

Le vamos a dar la palabra a Laureen Kapin para que haga la actualización sobre el trabajo que ha realizado este grupo hasta el momento. Gracias.

LAUREEN KAPIN: En primer lugar, bienvenidos a todos. Muchísimas gracias por sumarse a nosotros en esta enorme sala. Si quieren acercarse les prometemos que no vamos a ser agresivos ni feroces. Realmente les agradeceríamos que se sienten más cerca para que estemos todos un poco más unidos. Si no me oyen o tienen dificultades para entenderme, voy a tratar de hablar más fuerte o más despacio o más claramente.

Tenemos varias presentaciones y después de cada una de ellas tendremos un periodo de preguntas y respuestas pero si no tienen la posibilidad de hacer la pregunta ahora, por favor,

siéntanse libres de ubicarnos en forma individual y nosotros hablaremos con ustedes.

Bobby Flaim, mi colega, va a conducir la discusión de este tema junto conmigo. Vamos a estar controlándonos el tiempo así que vamos a comenzar. Una vez más, este es el grupo de trabajo de seguridad pública. Queremos comenzar dándoles un poquito de contexto. Si bien nuestro grupo de trabajo de seguridad pública es nuevo, las personas que han estado abogando por la seguridad pública han participado en este tipo de trabajo desde hace ya bastante tiempo, más de 10 años.

Durante ese tiempo hemos estado promoviendo distintas cuestiones. Por ejemplo, la creación de medidas de protección para los consumidores en el proceso de los nuevos gTLD. En ese sentido tenemos una expresión formal plasmada en el comunicado de Pekín, con un conjunto de salvaguardas aplicables a los nuevos gTLD basadas en el asesoramiento del GAC y en el trabajo reciente. También nos hemos focalizado en asegurarnos de que la junta directiva acepte implementar esas medidas de protección.

Esto ha estado ya en desarrollo durante un tiempo y Bobby va a hablar de algunas mejores en las disposiciones de los contratos.

ROBERT FLAIM: Cuando nos focalizamos en la creación del grupo de trabajo de seguridad pública, ustedes recordarán que había recomendaciones de los organismos de aplicación de la ley ya desde 2009 al 2013. Seguíamos trabajando en esa dirección con las especificaciones y con los grupos de trabajo. Hablábamos de la especificación de WHOIS, el grupo de trabajo de servicios de privacidad y proxy, o representación y otros temas que se vinculan con los nombres de dominio y con la seguridad pública. También ustedes podrán ver una mejora en la exactitud del WHOIS. Ese fue nuestro punto de partida en realidad.

Luego mis colegas aquí harán una explicación más detallada de por qué es tan importante la exactitud del WHOIS para el trabajo que nosotros realizamos como funcionarios de la seguridad pública y también cómo se puede lograr un equilibrio con las leyes de protección de datos europeas y también las políticas vinculadas con la seguridad pública en relación con la exactitud del WHOIS. Como ustedes saben, esto lo venimos haciendo desde hace 10 años y son temas que constantemente son parte de nuestro trabajo.

LAUREEN KAPIN: Lo que podemos extraer de esta primera sesión es que si bien bajo el Comité de Asesor Gubernamental somos un grupo de trabajo relativamente nuevo, hemos estado ya desempeñando

nuestras funciones en esta área durante mucho tiempo aunque ahora tenemos un canal más formal para comunicar todo este trabajo de incidencia bajo el paraguas del GAC.

El trabajo más reciente. Yo quiero que ustedes sepan que, como dijo Alice al comienzo, si les interesa ver la labor más reciente que hemos desarrollado, el sitio web del GAC es donde la van a hallar. Todos los grupos de trabajo del GAC de hecho tienen un espacio público en el sitio web del GAC. No es necesario ser miembro del GAC para poder acceder a esa información. Aquí tenemos el enlace a nuestro sitio en particular. El sitio web también incluye información sobre los representantes que conforman este grupo de trabajo y distintos comentarios que nosotros hemos presentado. Ese es el lugar al que tienen que recurrir si quieren leer por cuenta propia más información sobre nosotros.

Vamos a mostrarles las partes más destacadas del trabajo que hemos hecho en forma reciente. Bobby, ¿quieres hablar del RAA del 2013? Sé que es un tema que conoces muy bien.

ROBERT FLAIM: Sí, cuando se firmó el RAA de 2013 hubo algunos elementos que se desprendieron de ello y estableció las bases para el trabajo futuro. Una de ellas era la especificación de WHOIS y dónde se iba a hacer la revisión. Entonces ahora, este año, en el 2015, se

debatió cómo abordar la especificación de WHOIS que es parte del RAA y ver cómo se podía mejorar o cambiar. La ICANN y los registradores tenían algunas inquietudes. Había habido comentarios expresados. Se abrió, de hecho, un periodo de comentario público y el grupo de trabajo también hizo sus aportes a través de comentarios. Hicimos comentarios acerca del trabajo del grupo de trabajo de servicios de proxy y privacidad y también contribuimos desde el punto de vista del WHOIS de próxima generación que también estaba sometido a un periodo de comentario público.

Este grupo de trabajo de seguridad pública ahora es parte del GAC y se focaliza en estas cuestiones tan importantes. Si bien nosotros tenemos muchos representantes de los organismos de aplicación de la ley, nuestro grupo también estaba abierto a otros funcionarios gubernamentales como la agencia de Laureen que se ocupa de protección de los consumidores, la aplicación de medidas en el ámbito civil y también la FDA, por ejemplo, de Estados Unidos y sus equivalentes en otras partes del mundo. Ese tipo de organismos que pueden tener un impacto en la seguridad pública. Por eso van a ver que hay comentarios que se han elaborado a través de todos estos representantes en el grupo de trabajo.

Creo que lo que tenemos aquí en primer lugar es la revisión de la especificación de la exactitud del WHOIS. Antes de la reunión de

Buenos Aires, los registradores hicieron comentarios. De hecho, hicimos una sesión pública allí y nuestro interés era tratar de tener más especificidad sobre los comentarios que se expresaron. Hubo algunos plazos utilizados por los registradores y también un lenguaje calificador cuando se hablaba de sustanciar. Estábamos tratando de tener una definición un poco más exacta de qué estábamos hablando en esa especificación del WHOIS. Esto es algo que realmente sabíamos que íbamos a usar y que nos interesaba.

LAUREEN KAPIN: El RAA de 2013 tiene algunas obligaciones para los registradores. Tienen que verificar la exactitud de la información y hay un tiempo, un periodo durante el cual tienen que hacer esa verificación y actuar en ese sentido. Alguna de las preguntas en las que nos hemos focalizado tiene que ver con qué pasa si no tenemos una respuesta de la persona que se supone que tiene que dar esa información de contacto exacta.

Otra área en la que hemos presentado un comentario tiene que ver con los servicios de privacidad y de proxy y representación. Esto fue con el apoyo del grupo de trabajo que se ocupa de esa materia en particular. Este servicio esencialmente permite a las entidades enmascarar su información y puede haber motivos

por los cuales deban hacerlo. También pueden surgir inquietudes cuando eso ocurre.

El grupo de trabajo de seguridad pública presentó un comentario con respecto a algunas de las cuestiones que aparecían en el informe que se presentó. Pensábamos que tenía que hacerse una diferenciación entre la disponibilidad de esos servicios y más específicamente si hay un contacto por el cual se ofrecen servicios comerciales. Es decir, ustedes como consumidores, se les pide que otorguen su información financiera, número de tarjeta de crédito, información bancaria… En realidad tienen derecho a saber con quién están tratando. En consecuencias, los servicios de privacidad de proxy no deberían estar disponibles en ese tipo de situación.

También hacemos énfasis en la necesidad de la transparencia y la responsabilidad para los proveedores de servicios de privacidad y proxy. Cuando una entidad de aplicación de la ley hace una solicitud para saber quién está detrás de ese dominio que puede ser el objeto de la investigación, esas solicitudes tienen que manejarse de manera confidencial, según lo permitan las leyes locales porque los organismos de aplicación de la ley están interesados en que todos los hechos vinculados a esa investigación permanezcan confidenciales para que no se dé a conocer y no desaparezcan las pruebas y los distintos bienes. Perdón, no estaba tocando correctamente el botón. Aquí.

También hicimos comentarios sobre los servicios del WHOIS de próxima generación. Catherin va a explayarse más sobre este tema. Es una cuestión muy complicada en realidad que tiene que ver con lo que funciona y lo que no funciona ahora con WHOIS. Si debería haber un sistema subsiguiente y en ese caso surge toda una miríada de preguntas con respecto a cómo debería ser el sistema, quién debería tener acceso a la información. En nuestro comentario a este informe preliminar, lo que nosotros destacamos es que por un lado es complicado y por el otro tiene que haber un equilibrio que respete los derechos de los consumidores, mantenga la seguridad del público y también garantice la protección de los datos personales de los usuarios de Internet. Por lo tanto aquí abogamos por un equilibrio de todos estos distintos puntos de vista y que las comunicaciones se mantengan abiertas porque esto no es algo irreconciliable.

En Estados Unidos la Comisión Federal de Comercio se ocupa tanto de las cuestiones de consumidores, de protección de los consumidores, como de las cuestiones de privacidad, todo bajo el mismo organismo. No hay enemistades allí. Es importante tener un equilibrio entre estos dos aspectos. Este es el mensaje principal que tratamos de transmitir porque esa área es de suma importancia para nosotros.

ROBERT FLAIM: El representante de la Agencia Nacional del Crimen va a hablarles acerca de la especificación 11 que es el Marco de Seguridad del Acuerdo de Registros. Es algo que se originó del asesoramiento del GAC en Pekín hace unos dos años y medio. Jon ha estado trabajando con el grupo de trabajo junto con los registros para establecer prácticas voluntarias para tratar de ver cómo se podría trabajar ante estos casos de botnet, de phishing, de software malicioso, explotación infantil, para que tengamos un acuerdo cooperativo con los registros y podamos trabajar de manera eficaz con este tipo de delitos o abusos.

Esto es simplemente lo que les comento a modo resumido. Luego hablaremos más sobre este tema.

LAUREEN KAPIN: ¿Cuál es nuestro trabajo futuro? Nosotros esperamos tener la representación del grupo de trabajo que se ocupa de las cuestiones de competencia, elección del consumidor y confianza del consumidor que va a tener un papel crucial para considerar todos los aspectos en estas áreas. Además de la exactitud del WHOIS en relación con la información de los dominios, hay algo también importante.

ROBERT FLAIM: Sí. Hay algo más que es importante que es ver cuando buscamos los abusos y las atribuciones, también vemos en la otra cara del sistema del DNS que es el sistema de direcciones IP que esto es manejado por los RIR, por los registros regionales de Internet. Fuera de la ICANN, la ASO. Tenemos la organización de los recursos numéricos que está tratando también de trabajar en estas cuestiones con los acuerdos de acreditación de los registradores y se está pidiendo que hagamos lo mismo. Los RIR son cinco. Trabajamos con ellos para poder desarrollar y coordinar una política global con ellos para que todos tengan el mismo tipo de prácticas voluntarias que garanticen la exactitud del WHOIS y también el proceso de investigación de antecedentes o debida diligencia.

LAUREEN KAPIN: Con respecto al trabajo del grupo sobre seguridad pública, nos interesa tener mayor participación y colaboración también con otros grupos de trabajo dentro de la ICANN. Queremos extender nuestra llegada a otros actores gubernamentales, a todos los países que están presentes. Hay muchísimos organismos con personas que son sumamente conocedoras de determinados temas, gente que podría ser aliada para nosotros y servirnos de guía en nuestro grupo.

Por supuesto hay otras partes interesadas dentro de la ICANN que tienen muchísima información que para nosotros es sumamente valiosa. También vamos a tratar de llegar a ellos, acercarnos para poder beneficiarnos también de toda esa guía y esa sabiduría que existe en la comunidad de la ICANN. Esto es un pantallazo general del tipo de trabajo que hemos estado desarrollando en el grupo de trabajo. Esperemos seguir avanzando en el futuro. Quisiera saber si hay preguntas sobre estos temas que mencionamos porque este sería un buen momento para utilizar los micrófonos que están disponibles en la sala. Hay otras presentaciones pero nos pareció que era más organizado si tomábamos preguntas después de cada presentación.

ALICE MUNYUA: Muchas gracias, Bobby. Muchas gracias, Laureen. Hay dos micrófonos aquí al frente de la sala. Por favor, si tienen alguna pregunta. Por favor, diga su nombre.

VOLKER GREIMANN: Soy del Consejo de la GNSO, del grupo de partes interesadas de registradores. Nosotros, desde que existimos, venimos trabajando en el tema de la exactitud de WHOIS. Es una cuestión importante. Sin embargo, tiene el contrapunto de la cuestión de la privacidad. Quisiera saber si este grupo de trabajo con sus

antecedentes también puede lidiar o tratar con las implicancias de privacidad en materia de WHOIS para los usuarios de los nombres de dominio y ver cómo se puede proteger la privacidad de los datos de los registratarios.

¿Realmente un WHOIS público es lo que ustedes necesitan o es otro tipo de sistema lo que podrían necesitar?

ROBERT FLAIM: Creo que le van a responder muchas de esas preguntas cuando Catherin hable acerca de la protección de datos en Europa y otras cuestiones que generan desafíos en otras generaciones o en las próximas generaciones y lograr un equilibrio entre lo que funciona y lo que no. No quiero robarles su momento o su presentación o su momento de atención pero vamos a contestar su pregunta para abordar esas inquietudes.

ARTHUR ZONNENBERG: Hola, soy Arthur Zonnenberg. Trabajo para un registrador holandés acreditado por la ICANN. Aparte de este punto de la Unión Europea que comparto con Volker de cuáles serían las cuestiones a tratar por la Comisión Federal de Comercio en materia de privacidad y respecto de la Unión Europea, quisiera saber cuáles son los fundamentos, por ejemplo acerca de lo que ustedes hablaron con alguien da los datos de su tarjeta de

crédito. Bueno, eso les da derecho a saber quién está detrás del sitio web, con quién están tratando, y en el caso de un negocio en línea sería lógico para recibir un servicio pero si se trata de un activista que trabaja en contra de determinados intereses, por eso quiere mantener su privacidad.

Vamos a tener que respetar su privacidad para que se pueda respaldar a las personas que trabajan en pos de determinados intereses. Por supuesto que Estados Unidos siempre fue objeto o blanco de críticas porque siempre está en consonancia con estos intereses. Quisiera saber si el hecho de que yo les dé mis detalles de tarjeta de crédito me da derecho a saber sus detalles personales.

LAUREEN KAPIN: Bueno, quiero decir que hay diferentes opiniones acerca de esta cuestión. Desde el punto de vista de la protección del consumidor, si alguien está dando esos datos sensibles y por supuesto que usted tiene el derecho de estar en desacuerdo, nosotros consideramos que tenemos derecho a saber con quién estamos tratando. Entiendo las cuestiones sensibles que tienen que ver con los grupos que defienden determinadas causas. Pueden defender sus propios puntos de vista pero si tratan con información sensible, entonces nosotros consideramos que los consumidores, que el público tiene derecho a saber con quién

están tratando. Esa es una perspectiva. Somos conscientes de que no todo el mundo comparte este punto de vista.

GLORIA KATUUKU: No tengo una pregunta. Tengo un comentario. Esto deriva del GAC pero uno tiene aquí integrantes de los organismos de cumplimiento de la ley y hay integrantes en otros países que no han participado en estos procedimientos y quisiera que participen más. Soy Gloria. Soy de Uganda.

LEE HIBBARD: Hola, soy Lee Hibbard de Estrasburgo, del Consejo de Europa. Estoy en una organización que nuclea a 47 países. Tenemos la convención de Budapest y también tenemos cuestiones acerca de venta de medicamentos en línea, acerca del cuidado de la salud, acerca de farmacias en Internet. Quiero que el Consejo de Europa esté también en este mapa. Nosotros somos un miembro observador en el GAC y nos gustaría participar y colaborar con el conocimiento y la experiencia de los distintos grupos del Consejo de Europa. Tenemos mucho para compartir con ustedes y lo haremos en su lista de correo electrónico, donde ya hemos enviado comentarios.

En junio de este año, estos 47 países acordaron una nueva declaración sobre la ICANN, los derechos humanos y el estado

de derecho. Esto es para garantizar que la ICANN respete los procedimientos y los derechos humanos en sus políticas y procedimientos. Les voy a pasar todo esto a través de mi colega Peter que va a tomar la palabra.

PETER KIMPIAN: Hola, soy Peter. Buenas tardes. Represento al T-PD del Consejo de Europa. Es un organismo asesor de la convención 108. Estoy muy contento de estar aquí y también, al igual que mi colega, quiero ofrecer cooperación y colaborar con nuestro conocimiento y nuestra experiencia sobre protección de datos dentro de lo que sea posible. Creo que, como dijo nuestra colega de los Estados Unidos, la palabra correcta sería equilibrio. No hay cuestiones irreconciliables. Lo mejor y lo digo como funcionario que trabaja en una autoridad de protección de datos en la Unión Europea, lo mejor es sentarse a conversar abiertamente, a debatir preguntas y cuestiones y definir las mejores soluciones posibles. Estamos dispuestos a hacerlo. Estamos muy contentos de estar aquí y ofrecemos nuestro trabajo, nuestra energía, nuestro conocimiento y experiencia. Muchas gracias.

ALICE MUNYUA: Muchas gracias al Consejo de Europa. Vamos a tener una reunión con ustedes en el GAC.

DAVID CAKE: Quiero hacer dos comentarios. Uno específico y uno más general. El comentario específico es que recibimos sus aportes, sus comentarios en el grupo de trabajo PPSAI. Tengan presente que consideramos esto pero todo esto surgió cuando ya habíamos debatido estos temas en profundidad y tuvimos 60.000 respuestas del público en general. Sus aportes llegaron en una instancia tardía así que tienen esforzarse un poco más y participar en una instancia más temprana.

Entiendo que este es un grupo nuevo pero quería informarles de que quizás haga falta más participación de su parte. Luego tengo un comentario más general. Los organismos encargados de protección de datos y las leyes son leyes y tenemos estos organismos que se dedican a la seguridad pública y a la protección de datos pero brillan aquí por su ausencia en su grupo.

Consideramos que ellos tienen una voz muy contundente para ser oída aquí. Son una parte muy importante del cumplimiento de la ley así que es importante que ustedes sean percibidos como un grupo que representa todos los puntos de vista de los organismos de seguridad pública y cumplimiento de la ley. Con lo cual los aliento a que sean más inclusivos de forma activa,

sobre todo para incluir a los organismos que tienen que ver con seguridad pública y protección de datos.

ALICE MUNYUA: Muchas gracias, David. Nosotros no somos un grupo que hace lobby.

DAVID CAKE: Sí, sí, sí. Entiendo. Pero ustedes tienen que asegurarse de ser lo suficientemente inclusivos e incluir a todas las voces y tienen que ir a buscar esas otras voces.

ALICE MUNYUA: Nos tomamos muy en serio estos comentarios. Ayer hablamos acerca de esto cuando usted estuvo presente en los debates, en la GNSO, y sí, surgió el tema de que el GAC debe participar con mayor antelación, sobre todo en el PDP. A tal efecto estamos trabajando para lograr este objetivo pero también hay que entender cómo funcionan nuestros gobiernos. Tenemos que consultar en nuestras ciudades capitales, con nuestras partes interesadas. Pido disculpas si a veces nuestros comentarios llegan un poco tarde pero vamos a asegurarnos de trabajar en los procesos más de cerca para lo cual contamos con miembros que van a unirse a distintos grupo de trabajo para poder hacer

aportes de forma directa como grupo de trabajo del GAC. Gracias por sus comentarios.

DAVID CAKE: Entiendo que este grupo es relativamente nuevo y algunos de los grupos de trabajo son anteriores a ustedes, o sea que no tienen la máquina del tiempo para poder participar desde el principio. Los felicito por todo el trabajo del grupo de coordinación entre el GAC y la GNSO para que el GAC pueda participar más temprano en los PDP de la GNSO. La GNSO quiere recibir sus aportes y cuanto más temprano los recibamos, será mejor para todos, sobre todo los aportes del GAC, en especial los que tienen que ver con determinados temas. Si llegan rápidamente, lo ideal sería que llegasen después del informe inicial. Bueno, eso ayudaría a marcar el rumbo que puede llegar a tomar un grupo de trabajo. Sería más fácil y mejor para todos que esto sucediera con la debida antelación para poder ayudarnos a formular respuestas a nuestras conclusiones. Gracias.

ALICE MUNYUA: Gracias, David.

AMADOU LY: Buenos días. Soy Amadou Ly. Soy miembro del Colegio de Regulación de Telecomunicaciones de la República de Senegal. Los felicito y agradezco a todos los miembros del grupo de trabajo. Me hago muchas preguntas con respecto al tema de la seguridad y la confidencialidad, la seguridad de las informaciones, sobre todo en países como el mío, los países africanos como Senegal, donde hoy y hasta ahora hay personas que trabajan dentro de las administraciones y de los gobiernos que aún usan direcciones de correo electrónico genéricas (Yahoo, Gmai) y el nivel de Internet no es suficiente como para tener .gov en nuestros países.

Tenemos ejecutivos que trabajan en todas las administraciones y que usan correos electrónicos que tienen desde que eran estudiante, desde que empezaron a trabajar. Este tema es fundamental. Internet hoy ha llegado a un nivel insospechado. La gente trabaja con datos confidenciales, en las presidencias de repúblicas, en administraciones de alto nivel y no se dan cuenta de que están usando Yahoo, Gmail. ¿Podemos proteger a estas personas sin dejar de trabajar con las bases de datos? La gente que maneja base de datos muy importantes con datos muy confidenciales y no se dan cuenta de que están trabajando con datos muy importantes para los estados, información que está alojada en otros países porque no hay políticas de DSI o de gestión de mensajes, etc.

Esto es más evidente aún cuando vemos en las tarjetas de invitación de la gente que la dirección que usan es Yahoo o Hotmail. El tema es saber con quiénes trabajan ustedes. Hay que trabajar con esta gente que maneja datos importantes y que no está en un nivel suficiente. Esta es la responsabilidad. ¿Dónde está el límite o el trabajo que ustedes pueden hacer conjuntamente para poder aportar seguridad? Porque podemos crear firewalls, todo lo que uno quiera, pero si a nivel de las base de datos no estamos seguros de las transacciones, no sabemos cuál es el encaminamiento de la información, en ese caso me parece que hay un gran problema en mi opinión que necesita mucha más reflexión y trabajo en común con las diferentes personas y actores que interactúan para que los datos puedan seguir su tránsito. Muchas gracias.

LAUREEN KAPIN: Creo que usted planteó cuestiones muy importantes y definitivamente hay que hacer una tarea de educación, de formación, para que el público sepa cómo estar seguro en Internet y cómo considerar correo electrónico de Gmail o de Yahoo, e incluso si alguien dice que son del gobierno.

No voy a poder responder todas las preguntas que usted ha planteado porque son preguntas muy complejas pero sí sé que hay una necesidad real de educar al público para que sea muy

cauteloso al utilizar Internet, ya sea porque están comprando un producto, porque están en un sitio de citas en Internet, porque han recibido un correo electrónico que les dice que han ganado un concurso o porque alguien está enamorado de ellos y necesita dinero en efectivo con suma urgencia. Todas estas son cuestiones muy importantes que tenemos que tener presentes y sobre las cuales tenemos que trabajar porque realmente la vida de las personas puede verse afectada de una manera sumamente negativa y dañina por quienes se quieren aprovechar de ellos en Internet.

ALICE MUNYUA: ¿Alguna otra pregunta?

AMADOU LY: Muchas gracias por esta pregunta. Lo que yo me pregunto aquí es cómo nosotros en ICANN trabajamos con los grandes actores: Google, las grandes empresas que manejan las bases de datos. ¿Qué hacemos con ellos en forma general para tratar de hacer que el manejo de estas bases de datos sea más seguro? Estoy de acuerdo con usted en que las personas que las manejan son responsables de sus actos pero creo que también hay una responsabilidad de parte de todas las grandes empresas que manejan las bases de datos y que también albergan las transacciones.

Estoy de acuerdo con usted en que hay que estar alerta pero quisiera saber cuáles son las medidas que podemos tomar o que podríamos llegar a tomar para tratar de asegurar estas transacciones. Esta era la intención de mi pregunta.

ALICE MUNYUA: Bueno, tenemos que pasar ya a la siguiente sección así que muchísimas gracias por estos comentarios. La colega de la Comisión Europa, Catherin, va a hablar justamente de alguno de estos temas. Va a hablar de WHOIS, de las leyes de protección de datos y seguramente allí tendremos varios ejemplos que nos muestren cómo abordar este tipo de temas en algunos países africanos y también en otras partes del mundo. Catherin tiene la palabra.

CATHERIN BAUER-BULST: No sé cómo le puedo dar soluciones para todo el mundo pero realmente me gusta ver que hay interés en este tema. Como ya dijo Laureen, es necesario llegar a un equilibrio y, en mi experiencia en este tipo de debates siempre ha habido un beneficio cuando se comienza por una base de evidencia sólida. Quisiera hacer una introducción muy breve sobre las normas de la Unión Europea que rigen la protección de datos y las implicancias que estas tienen para procesos como, por ejemplo, el rediseño del WHOIS.

Cuando me preparaba para armar esta presentación, empecé a ver hacia atrás la historia de larga data del WHOIS, toda la discusión en términos generales y ahora hablamos mucho de responsabilidad y en realidad esta responsabilidad, que la necesitamos, también es un tema que tratamos desde hace muchísimo tiempo. Ya hace 2.000 años en la República de Platón se hablaba de la responsabilidad y allí estaba la historia de un pastor que estaba rodeando una colina con su rebaño y llega a una cueva donde encuentra un anillo y cuando se lo coloca se torna invisible. Por esta invisibilidad va a la corte, mata al rey, tiene relaciones con la reina y toma posesión del gobierno.

En esta obra de Platón, la parábola es que aquí hay una cuestión de rendición de cuentas, de responsabilidad. Platón y sus amigos llegaron a la conclusión de que la responsabilidad es una sensación de una construcción moral. Cuando a uno le sacan la habilidad de los otros de verlo, entonces ya no hay un incentivo para seguir actuando de manera responsable. Justamente hablamos de este tema a raíz de esta parábola y esta historia del anillo de Giges, de este pastor.

Creo que no necesariamente nosotros tenemos que hacer aquí una concesión recíproca. Yo trabajo en el ciberdelito y de hecho yo estoy a la vanguardia de la defensa de la protección de los datos porque quiero evitar que se roben las identidades, los

datos, las credenciales, las imágenes de niños que se utilizan para delitos de abuso sexual y estamos trabajando para permitirles a los organismos de aplicación de la ley prevenir este tipo de delitos y proteger a aquellos que sufren, que son víctimas de ellos.

Quiero representar ambas visiones aquí. Voy a hacer una recapitulación breve con respecto a lo que los organismos de aplicación de la ley tenemos como interés central. En la afirmación de compromisos de la ICANN se asume la obligación de mantener un acceso público y restricto y oportuno a información de WHOIS completa y exacta. Aquí es necesario revisar la eficacia de la política del WHOIS cada tres años. El GAC en el comunicado del 2007 estableció algunos principios con respecto a lo que debía ser WHOIS para ayudar a la aplicación de la ley y en las investigaciones y también para ayudar a aplicar las leyes nacionales e internacionales, para combatir los usos abusivos y también para ayudar a las empresas y a otras entidades a combatir el fraude y salvaguardar los intereses del público.

Volvamos a los aspectos fundamentales, ahora desde la perspectiva europea. La protección y la seguridad de los datos son derechos fundamentales que están en la carta orgánica de la Unión Europea en los artículos 6, 7 y 8, que básicamente indican que todos tienen el derecho a la libertad y a la seguridad

y que todas las personas tienen el derecho a ser respetados en su vida privada y familiar, en sus hogares y en sus comunicaciones.

Esta carta de la Unión Europea es moderna en el sentido de que contiene derechos pertinentes a la sociedad digital, garantiza la bioética y la transparencia pero también es más específica respecto a la protección de los datos. En el artículo 8 hace referencia al derecho de protección de los datos personales. Dice que se deben procesar de manera equitativa y que todos tienen derecho a acceder a datos que han sido recabados sobre su persona y para asegurarse de que esos datos sean exactos. Estos son derechos clave en una sociedad democrática y no son absolutos. Cada uno de estos derechos, el derecho a la seguridad, a la privacidad y a la protección de los datos tienen que equilibrarse entre sí y también con otros derechos fundamentales.

Ahora quiero brevemente resaltar las disposiciones más importantes de nuestra directiva que es el texto jurídico más importante con respecto a la protección de los datos en la Unión Europea. Esta directiva hace referencia a la protección de los individuos con respecto al procesamiento de sus datos personales. Hemos escuchado muchas inquietudes, muchas preocupaciones en el pasado, sobre el hecho de que no había una voz unificada en Europa en este tema, los requerimientos de

protección de datos. El tema principal aquí es que la base de todo era una directiva que es un tipo de instrumento legislativo especial que es vinculante en cuanto a sus metas pero que deja que los distintos estados miembro decidan cómo desean implementarlo con su propia legislación nacional para alcanzar esas metas.

Esto significa que no tenemos un único conjunto de leyes idénticas sino que tenemos 28 conjuntos de leyes diferentes pero el objetivo es que todos apunten al mismo objetivo aunque no contengan exactamente la misma redacción. Esto es todo un desafío. Estamos trabajando para aprobar una nueva legislación sobre la protección de datos. Esperemos que la aprobemos a fines de este año como reglamentación, como regulación, para que ya no se necesite implementar la ley de manera diferente en los distintos estados miembros sino que se pueda aplicar por sí misma en su propio derecho. En cierta forma podemos tener respuestas más coherentes de los países europeos sobre algunas de estas cuestiones una vez que se haya implementado este instrumento.

Quiero explicar brevemente la definición de datos personales que utilizamos en la Unión Europea. Es toda información relacionada con una persona natural identificable o identificada. No se habla de la sensibilidad de la información aquí. El único factor fundamental aquí es si uno puede

identificar o no a una persona. Un nombre es datos personales, una dirección de IP también puede ser considerado un dato personal. En el ejemplo de la Unión Europea, por ejemplo, un multiciudadano que trabaja para la Comisión Europea en un determinado lugar también puede ser considerado como un dato personal porque es algo que permite identificar a esa persona cuando tiene un determinado número para actuar en esos organismos dentro de la Comisión Europea.

No importa si la información es sensible. El concepto de datos personales no diferencia entre el contenido o los datos que son transmitidos o la información del suscriptor. Tienen que ser datos personales. Hay otro concepto clave y que aquí ya lo han mencionado. Todo lo que se hace con los datos es procesarlos, ya sea que ustedes lo miren, que lo almacenen, que lo eliminen, que lo trasladen, que lo divulguen, todo corresponde a lo que nosotros consideramos procesamiento.

Cuando se recopilan datos para procesarlos tienen que tener un motivo específico. La cantidad de datos tiene que ser pertinente para esos fines que uno persigue y no ser excesiva. También la información tiene que ser exacta y actualizada. No se puede guardar más tiempo de lo necesario y todo el ejercicio tiene que estar legitimado por un fundamento legítimo. Es decir, la persona que es propietaria de esos datos dio su consentimiento porque se necesitan para celebrar un contrato o algunos otros

motivos. ¿Quiénes son los actores para la protección de los datos? Yo estaba hablando de la aprobación de las regulaciones. Eso será aprobado por el Parlamento Europeo y el Consejo de la Unión Europea que son los actores legislativos.

Yo vengo de la Comisión Europea que está a cargo de proponer la legislación y monitorear, supervisar su implementación. Luego tenemos las autoridades de protección de los datos a nivel nacional que estarán a cargo de supervisar la implementación de la protección de los datos a nivel nacional y luego el grupo de trabajo artículo 29, seguramente ustedes lo habrán escuchado nombrar porque hizo comentarios en distintos procesos, son un grupo de trabajo que reúnen a todas las autoridades vinculadas con la protección de los datos a nivel nacional y la comisión en una función de asesoramiento. Básicamente dan asesoramiento a la comisión y a otros sobre cómo se deben implementar las leyes de protección.

Luego tenemos la Corte de Justicia de la Unión Europea que es el único órgano autorizado para interpretar las leyes en materia de protección de los datos. Son los que nos dan las respuestas con respecto a la implementación de la reglamentación en materia de protección de los datos.

¿Qué significa esto desde el punto de vista del WHOIS? Estamos rediseñando el WHOIS. Hay tres aspectos centrales que tenemos

que tener en cuenta desde el punto de vista de la protección de los datos y de la aplicación de la ley. Por un lado la disponibilidad. Como acabamos de enterarnos, estos datos tienen que estar recopilados para un fin legítimo, con un fundamento también legítimo, por ejemplo el consentimiento de la persona que es sujeto de esos datos y cualquier servicio futuro de directorio de registro también tiene que asegurarse de dejar bien en claro cuál es el objetivo, para qué fin va a utilizar esos datos porque aquí también hay un componente de rendición de cuentas, de responsabilidad. No debe recolectar más datos de los que se necesitan para ese fin y no debe guardarlos durante más tiempo del necesario.

Ahora, el acceso. El hecho de que esto sea un sistema público y que la ICANN en su afirmación de compromisos se ha comprometido a conservarlo de esa manera, este es un tema central. Desde el punto de vista de la protección de los datos, la directiva no dice nada con respecto a limitar el acceso a los datos pero obviamente si pensamos en el espíritu de la ley, sería muy útil si los datos no se divulgaran de manera innecesaria.

Con respecto al componente de exactitud, esto es bastante sencillo porque justamente cuando hablamos de los organismos de aplicación de la ley y quienes entienden en materia de protección de los datos, todos estamos alineados aquí. Todos queremos que los datos sean exactos. Eso es todo lo que yo

tengo para compartir con ustedes y con gusto voy a responder sus preguntas. Muchísimas gracias.

ALICE MUNYUA: Gracias, Catherin. ¿Hay alguna pregunta o comentario? Por favor, acérquense al micrófono para hacerlos.

Entonces tal vez podamos avanzar a la siguiente presentación donde veremos algunos ejemplos del WHOIS. Greg será quien lo presente, del Centro de Ciberdelitos Europeo.

GREGORY MOUNIER: Les pido por favor que pongamos la presentación en pantalla.

ALICE MUNYUA: Hay una pregunta. Preséntese, por favor.

VOLKER GREIMANN: Soy del grupo de registradores del consejo de la GNSO. Quisiera agradecerles por esa presentación tan interesante y tan concisa sobre la posición europea con respecto a la protección de los datos. Para muchos de nosotros desde el principio ha quedado claro que el WHOIS tal como está ahora tiene muchísimos datos privados de millones de ciudadanos que se publican a diario y esto realmente es problemático desde el punto de vista de la protección de los datos de Europa y también de otros países.

Necesitamos una revisión clara y bien definida del WHOIS tal como está ahora para asegurarnos de que estos datos no estén más disponibles libremente como lo están ahora. ¿Estarían de acuerdo con eso? Desde el punto de vista del grupo de trabajo de seguridad pública, ¿cómo debería implementarse ese tipo de régimen?

CATHERIN BAUER-BULST: Estoy de acuerdo con usted en que lo ideal sería que no hubiera un acceso abierto total a todos los datos que están ahora disponibles. ¿Pero cómo se equilibra esto en la práctica con la función que tiene que cumplir el WHOIS? En la Unión Europea también hay legislación que exige de hecho que se publique la información en los sitios web. Por ejemplo, para todo actor que no está actuando a título personal, es decir, que no está simplemente publicando sus propias fotografías sino que pone las de su familia, de sus amigos, en ese caso tiene que cumplir con la obligación del WHOIS y tiene que poner en su sitio web la información detallada de contacto para poder asumir cualquier responsabilidad en caso de que se considere que ha cometido algo que es ilegal.

Es difícil lograr este equilibrio. En estas circunstancias no estoy segura de que exista un sistema perfecto. Creo que no podemos llegar a ese punto pero hay que considerar las inquietudes de

ambas partes y tratar de conciliarlas, pero lamento que no tengamos una solución perfecta.

VOLKER GREIMANN: Entiendo que no hay una solución perfecta. Continuando en la misma dirección, cuando ustedes presentan este tema, es importante que diferencien el contenido que aparece en un sitio web donde se necesitan algunos requisitos de apertura y que pueden ser beneficiosos para que no vaya a las direcciones privadas de los particulares, por ejemplo. Por ejemplo, para las registraciones de los nombres de dominio que tal vez se utilicen para enviar correos electrónicos donde no hay publicación alguna al mundo externo pero están allí obligando a los registradores a publicar sus detalles privados.

También me gustaría que vean cómo algunos registros europeos están manejando y publicando los datos de WHOIS, lo que está haciendo Nominet, lo que hacen otros registros en el espacio europeo, la cantidad de datos que están visibles, a la vista del público porque es muy limitada, tal vez limitada al nombre y a una dirección. A veces ni siquiera la dirección de email se publica. Es importante que vean esto para formar un modelo para la presentación de los datos privados cuando se presentan en el contexto de la ICANN.

ALICE MUNYUA: Por favor, preséntese. David.

DAVID CAKE: David Cake, de Australia. Miembro del Consejo de la GNSO. Una vez más tengo un comentario general y algo específico. En términos generales creo que fuera una presentación muy buena. Muchas gracias. Creo que subraya la necesidad de pensar en las distintas piezas que conforman el WHOIS, los principios a los que debemos adherirnos a largo plazo y también los requisitos transitorios que tal vez puedan cambiar porque considero que sería así. Lo vi esta última semana en los sitios web que empezaron a hablar de que iban a ser dados de baja porque no cubrían todos estos requerimientos.

Creo que tenemos que ser flexibles y lograr un equilibrio entre aquellas cosas que no cambian y aquellas que sí cambiarán. Hablando de aquellas que sí van a cambiar, tenemos los servicios de directorio de registros, el PDP correspondiente a esos servicios que se desarrollará el año próximo en la GNSO. Va a haber un esfuerzo muy grande para ver y responder a todas las preguntas con respecto a quién tiene acceso a esos datos, qué datos se recaban, quién los ve y es importante que haya participación a través del periodo de comentario público respondiendo a nuestras publicaciones en forma de comentarios.

También si trabajaran con el grupo de trabajo artículo 29 o con una entidad similar que tenga un conocimiento bien profundo de las cuestiones de protección de los datos, eso realmente sería muy valorado porque nos daría una buena orientación, se podrían responder preguntas muy específicas. Sugiero que también tengan la participación de personas con ese tipo de perfil. A partir del interés de alguien de la GNSO que tal vez podría participar, creo que en ICANN necesitamos encontrar a esta gente que tiene estos conocimientos tan especializados sobre la privacidad de datos como la gente que está en artículo 29 y gente de ese estilo.

ALICE MUNYUA: Por eso el GAC desarrolló este grupo de trabajo. Ciertamente nos vamos a asegurar de participar específicamente en alguno de estos procesos y en las etapas tempranas. Muchísimas gracias. Preséntese.

KIRAN MALANCHARUVIL: Yo soy Kiran Malancharuvil. Con respecto al grupo de partes interesadas de los registros, creo que aquí han presentado algunas posiciones que se contraponen con lo que se dijo en los comentarios al grupo de trabajo de servicios de privacidad y proxy. Creo que tiene que ver con la especificación de la

exactitud del WHOIS donde se alienta el acceso abierto a la información del WHOIS para esos campos de datos.

Me gustaría que haya una explicación o una aclaración porque me parece que hay algunas cosas que usted dijo que son contradictorias con lo que esos grupos están proponiendo.

CATHERIN BAUER-BULST: ¿Se refiere a mí? Muy bien, no me había dado cuenta. No estoy segura de dónde se produce la contradicción. Lo que yo estaba tratando de presentar son dos perspectivas diferentes. Por un lado la situación ideal desde la perspectiva de la protección de los datos y por el otro la situación ideal desde el punto de vista de los organismos de aplicación de la ley. Como dije al comienzo de mi exposición, hay derecho a la seguridad y derecho a la privacidad que son considerados derechos fundamentales desde el punto de vista de la Unión Europea y también en otras regiones del mundo. Ninguno de estos derechos se otorga de manera absoluta.

En la práctica, lo que se está tratando de hacer es lograr un equilibrio. Eso es lo que tenemos que hacer en este proceso de desarrollo de políticas. Muchísimas gracias nuevamente por la invitación al representante del grupo de trabajo artículo 29 para que nosotros participemos. Me voy a asegurar de transmitir esta información en Bruselas y que mis colegas también contacten

con ustedes. Me voy a asegurar de que ellos sepan que ustedes quisieran contar con su participación.

En este proceso esperamos que se pueda lograr el equilibrio adecuado entre estos dos derechos fundamentales. Ninguno tiene prevalencia sobre el otro así que creo que no hay una contradicción aquí.

KIRAN MALANCHARUVIL: Creo que sería útil esa participación que podrían tener en ese grupo de trabajo y tal vez en la redacción de los comentarios públicos que se obtuvieron a través del grupo de seguridad pública. Podemos tener un ejemplo de lo que usted nos indica como la necesidad de lograr un equilibrio entre estos derechos porque obviamente tenemos apertura en la información del WHOIS y tenemos que asegurarnos de que haya un equilibrio adecuado con los intereses legítimos de privacidad también. Creo que no hay que hacer declaraciones absolutas sobre la apertura de WHOIS y sobre esto así que le agradezco la aclaración.

CATHERIN BAUER-BULST: Sí, entiendo su preocupación y estoy reflejando la política actual tal como está ahora desde la perspectiva de los organismos de aplicación de la ley. Si no tratáramos esta apertura del acceso

sería muy difícil hacer algo más. Tenemos que concentrarnos en este proceso de desarrollo de políticas con mucho cuidado.

ALICE MUNYUA: Le doy la palabra a Greg.

GREGORY MOUNIER: Muchas gracias. Les voy a dar algunos ejemplos de la utilidad de WHOIS en algunas investigaciones o para algunos investigadores. Voy a hablar desde el punto de vista de los organismos de aplicación de la ley. Les cuento acerca de la agencia de cumplimiento de la ley en Europa. Nosotros trabajamos en respaldo a 28 estados miembro y también a fuerzas policiales y organismos de cumplimiento de la ley. Nosotros creamos este centro de ciberdelito europeo en 2013 y nos basamos en información que obtenemos por parte de los estados miembro, de nuestros socios.

En el ciberdelito trabajamos con el Reino Unido, trabajamos con el FBI, por ejemplo, de los Estados Unidos. En cuanto al ciberdelito tenemos tres grupos operativos. En primer lugar tenemos uno que se encarga de fraude online o en línea. Luego tenemos el que se encarga de la explotación sexual infantil en línea y luego el tercero que se encarga de los ciberataques que atacan a los sistemas de información y tiene que ver con

malware y botnets para hacer ataques al sistema bancario, por ejemplo.

Se me pidió que diera algunos ejemplos para darles alguna idea de la utilidad del WHOIS para los investigadores en el ciberdelito. Hay muchos factores en juego cuando uno trata de resolver un caso donde hay un ciberdelito pero en última instancia todos sabemos que hay muchos productos y servicios en línea que están muy fácilmente disponibles, que uno los puede comprar ocultando su verdadera identidad. No tiene sentido que los enumere a todos ahora pero en este contexto el rol del WHOIS es crítico. Es una de las herramientas entre tantas que tienen los investigadores de ciberdelitos para poder ver quién es el culpable de un crimen o de un delito.

Los delincuentes se protegen detrás del anonimato pero si tenemos un WHOIS con datos del usuario que estén validados y sean exactos podemos disminuir las posibilidades de que los ciberdelincuentes puedan ocultar su identidad. Tenemos que lograr esto de manera tal que los ciberdelincuentes tengan que recurrir a técnicas más complejas para ocultar su identidad o sus rastros.

Primero tenemos un caso de un botnet. Supongo que todos ustedes están en cierto modo familiarizados con un botnet que es una red de computadoras infectadas por software malicioso

que permite que un delincuente controle esa red de computadoras y utilice un comando de manera tal que las computadoras luego hagan varias actividades ilícitas o delictivas. Nosotros vemos cuál es el último de los servidores que tuvo comunicación en esta botnet. En lo que tiene que ver con los usos abusivos o indebidos del DNS vemos que si alguien logra mantener una cadena de nuevas registraciones de nuevos dominios, entonces se logra tener una botnet o una red de software malicioso muy efectiva.

Si tenemos nombres de dominio de registradores de todo el mundo con rapidez no solo se pueden sostener las solicitudes de baja de servicio sino también otros intentos de afectar la red o de tomar la red por parte de otras personas. Tenemos esta técnica del DNS que es de suma utilidad para el tema de las botnet.

Cuando se me pidió que viniera aquí a hablar con ustedes, consulté a un equipo de investigadores porque yo soy simplemente un asesor de políticas y trabajé con ellos. Vimos una serie de casos desde el punto de vista del WHOIS y del DNS y hubo un caso, un operativo muy reciente en el cual el equipo que se encarga de estos temas tuvo que controlar un botnet que se dedicaba a software malicioso que atacaba a sistemas bancarios online. Hubo una comunicación con uno de los sospechosos en los cuales se compartieron detalles del dominio

en cuestión. Hicieron una búsqueda de WHOIS sobre ese dominio y ahí obtuvieron un correo electrónico utilizado para registrar el dominio. Luego hicieron una búsqueda inversa o reversa de WHOIS de ese correo electrónico y encontraron otros dominios registrados con el mismo correo electrónico.

Entre esos nombres de dominio había un dominio creado por este individuo en cuestión hace unos años y lo había utilizado para crear un perfil profesional con su currículum, con su foto, etc. antes de ser un ciberdelincuente. Cuando utilicé esos detalles personales, nosotros pudimos encontrar una base de datos en un país donde vivía esta persona y vimos que esa era su verdadera identidad. Entonces demostramos que esa persona de hecho era un ciberdelincuente y así pudimos iniciar acciones legales con éxito.

Si tenemos datos exactos, podemos encontrar al culpable de un delito con mucha más rapidez o celeridad. Les doy otro ejemplo de un caso de un botnet que distribuía webinjects que es un ejemplo negativo. Uno de mis colegas dedicó tres meses a estudiar a un ciberdelincuente que se dedicaba a desarrollar webinjects para atacar a clientes del sistema bancario. Una vez que la víctima estaba infectada por este software malicioso, iniciaba sesión en su portal de banca en línea, de operaciones bancarias en línea, y llegaba a un dominio que lo mandaba a un sitio web del ciberdelincuente que era muy similar al sitio

verdadero. Cuando la víctima ingresaba sus credenciales o sus claves de acceso, estas eran captadas por el ciberdelincuente.

Mis colegas en los últimos tres meses vieron que el sospechoso había registrado 18 dominios distintos, todos con webinject apuntando a personas en Reino Unido, Países Bajos y Alemania. Tenía cuatro conjuntos de identificadores para identificar todo esto y para registrar esto: correos electrónicos, nombres, números de teléfono.

Se trabajó en cada uno de estos identificadores y como resultado se llegó a muchos otros identificadores. En ninguno de ellos pudimos obtener una identidad real pero si hay un ciberdelincuente que trabaja “correctamente” entonces uno dedica un tiempo muy valioso de investigación a perseguirlo en vano. Mis colegas dedicaron tres meses y no pudieron detectar esa identificación porque los identificadores no eran legítimos pero habían sido obtenidos de una botnet. Entonces si en aquel momento el registrador hubiera validado esos identificadores, entonces quizás mis colegas no habrían desperdiciado su tiempo y hubieran dedicado su valioso tiempo a investigar otros casos.

Este es un ejemplo de cuando no tenemos los datos exactos o precisos y de cómo perdemos nuestro tiempo. No voy a hablar acerca de este caso. Esta es una botnet muy famosa que surgió

en febrero. Dedicamos muchísimo tiempo, malgastamos muchísimo tiempo porque no teníamos datos exactos de WHOIS de la persona que estábamos persiguiendo pero contarles algo positivo. Este es un caso de explotación sexual infantil. Estos son sitios web que están en manos de criminales en la web abierta, no en la web oscura o dark web o web oculta.

Lo que hacen es vender material de pornografía infantil en línea. Por 99 dólares por mes, los clientes tienen acceso ilimitado a material de pornografía infantil. Lo que hicieron mis colegas fue ver esos sitios web y recopilar los nombres de dominio de esos sitios web utilizando diversas técnicas. Luego juntaron la información del DNS asociada a esos nombres de dominio. Es decir, las direcciones de IP con herramientas disponibles para los registradores y para cualquier investigador. Luego tuvieron un conjunto de datos de WHOIS asociados a estos nombres de dominio.

En teoría, lo que tenemos es el dominio A que tiene información específica del DNS que indica que está relacionado con una relación IP A. El dominio B tiene información que indica que está ligado al IP B. No hay vínculo entre los distintos dominios, pero al hacer una referencia cruzada entre los tres conjuntos de datos: información de DNS, nombre de dominio y datos de WHOIS, se puede encontrar una dirección de correo electrónico válida en común en todos estos nombres de dominio que fue

utilizada por el registratario para registrar los dominios. Utiliza un solo correo electrónico para comunicarse con el registrador para la facturación.

Como conclusión, se pudo arrestar a un grupo de delincuentes y se pudo dar de baja a esos sitios web. Desafortunadamente, este es un negocio tan bueno que siguen surgiendo este tipo de sitios. Como conclusión quiero reiterar lo que dije previamente. Los datos confiables y precisos de WHOIS son sumamente importantes para que los organismos de cumplimiento de la ley puedan combatir el ciberdelito pero si alguien es un muy buen ciberdelincuente se podrá salir con la suya pero se ahorra un valioso tiempo de investigación que hace que la vida de los ciberdelincuentes sea más difícil y para eso estamos los organismos de cumplimiento de la ley.

ALICE MUNYUA: Muchas gracias, Greg. Tenemos participantes remotos. Olof, de la secretaría del GAC las va a leer para los panelistas.

OLOF NORDLING: Habla Olof Nordling, del personal de la ICANN, personal de apoyo para el GAC. Tenemos una pregunta de un participante remoto que se llama Michael Ilishebo. Es un fellow de la reunión ICANN 52 y trabaja para la policía de Zambia. Dice: “WHOIS es

una herramienta poderosa para una investigación de ciberdelito. Sin embargo hay fallas por parte de los registratarios que normalmente no dan nombres y direcciones exactos al registrar un sitio web y por lo tanto es difícil hacer una investigación. ¿Hay alguna manera en que los registratarios puedan garantizar que solamente…?" Disculpen, se me borró la pantalla.

Repito la última parte: "¿Hay alguna manera en la cual los registratarios puedan garantizar que solamente se aceptarán detalles o información verdadera durante el proceso de registración? Además, ¿cuánto avanzó Europol para garantizar que los programas de creación de capacidades sobre ciberdelitos sean introducidos para los organismos de cumplimiento de la ley en África?"

ALICE MUNYUA: Muchas gracias. ¿Alguno de los miembros del panel desea responder?

GREGORY MOUNIER: Con respecto a los programas de creación de capacidades de Europol, desafortunadamente no estamos participando en esos programas. Respaldamos las investigaciones de los estados miembro. Creo que tenemos un portfolio mucho más amplio.

Interpol tiene un portfolio mucho más amplio para respaldar a las comunidades en África. Creo que mis colegas tienen algo para decir.

CATHERIN BAUER-BULST: Nosotros tenemos ese tipo de programas de creación de capacidades para los países africanos y tenemos nuevas oportunidades de fondos, sobre todo para los países africanos. Estamos viendo eso dentro del área de creación de capacidades en materia de ciberdelitos.

ALICE MUNYUA: Lamentablemente se nos está acabando el tiempo. Hay cinco personas que quieren formular preguntas. Les pido que sean breves para que el resto de los panelistas puedan dar sus presentaciones. Muchas gracias.

ELLIOT NOSS: Elliot Noss de Tucows. Muchas gracias por haber respondido dos de mis cinco preguntas. Primero ustedes han hecho un muy buen trabajo al detectar la mayor fortaleza para las investigaciones. Todos sabemos que los criminales o los delincuentes a veces cometen un error tonto y eso sucede en los negocios también. La gente que comete un error tonto no

permanece en el mercado y es reemplazada por gente más inteligente.

Al tratar con la comunidad que se dedica a la seguridad hay que hablar con ellos acerca de su experiencia con los registradores y con ese intercambio con los registradores para obtener información. ¿Lo han hecho?

GREGORY MOUNIER: Bueno, no hablé acerca de la relación con los registradores pero los investigadores me dicen que en general si tienen una buena relación con un registrador, suelen obtener una cooperación mucho mejor que cuando esa relación no es tal. Estamos educando a los investigadores a nivel interno para forjar una relación positiva con los registradores y con el sector privado que muchas veces tiene las herramientas para resolver una investigación de un ciberdelito, de manera tal que el sector privado sepa cuáles son nuestras limitaciones, qué es lo que queremos obtener y nos dé la información que necesitamos.

ELLIOT NOSS: Creo que eso es alentador. No tiene que ser solamente una relación personal. Hay muchos datos que son muy valiosos para una investigación. En segundo lugar, no vi…

ALICE MUNYUA: Elliot, lamento interrumpirlo pero nos quedan 10 minutos. Lamento interrumpirlo. Voy a pedirle al resto de las personas que también nos envíen las preguntas después de la sesión porque nos estamos quedando sin tiempo. Muchas gracias. Por favor, formule su pregunta pero la responderemos más tarde.

ARTHUR ZONNENBERG: Muchas gracias por su presentación. Estoy tratando de entender lo que ustedes han descrito acerca de los errores tontos que cometen los ciberdelincuentes. Comprendo también lo que se ha dicho acerca de la dirección de correo electrónico y la importancia de la misma pero, por ejemplo, si alguien le roba la identidad a Catherin y tiene una copia de su pasaporte, yo, como registrador, ¿cómo sé que no se trata de Catherin, que no es ella la que lo está haciendo?

Lo único que puede hacer es preguntarle si ella registró tal o cual nombre de dominio y generalmente contactamos a las personas por teléfono pero puede haber alguien que conteste el teléfono y me diga: “Sí, sí. Soy Catherin”. Por supuesto, yo no sé quién es Catherin. ¿Cómo creen ustedes que yo puedo validar lo que estoy haciendo para verificar la identidad mediante varios métodos que no voy a divulgar? Por otra parte, no tengo ningún problema con que ustedes tengan mis datos pero sí que mis

oponentes políticos obtengan mis datos si yo soy activista respecto de una causa política. Gracias.

ALICE MUNYUA: No vamos a responder a las preguntas ahora. Pueden seguir formulando sus preguntas. Las vamos a responder más adelante porque tenemos dos presentaciones pendientes.

ASHWIN SASONGKO: Hola, soy Ashwin de Indonesia. En Europa tenemos un concepto que es "Conozca a su cliente". Es decir, un banco debe saber exactamente quién es su cliente y ver su documento de identidad europeo, por así decirlo. Lo mismo cuando uno quiere un correo electrónico. Hay que saber quién está detrás y si una compañía quiere tener un sitio web, hay que saber quién es la persona de contacto técnico y dónde están sus oficinas. Gracias.

PETER KIMPIAN: Tengo una pregunta que es la siguiente. Quizás es importante enfatizar que Europol está trabajando junto con un régimen exhaustivo de protección de los datos de muy alto nivel sobre todo en EC3. Hay un grupo de Europol que está investigando el tema de protección de datos, todo el procesamiento de datos dentro de Europol, o sea que tienen mucho conocimiento, mucha experiencia y retomo lo dicho previamente. Hay mucho

conocimiento en Europol y a nivel europeo que puede ser valioso en los organismos de cumplimiento de la ley y en toda la estructura de nuestro sector a futuro.

WANAWIT AHKUPUTRA: Creo que tenemos que seguir avanzando. Le voy a dar la palabra ahora al representante del Reino Unido. PSWG ha empezado a innovar y a trabajar y van a compartir con nosotros la labor que están haciendo y que han hecho en su país. Le damos la palabra a Nick Shorey en primer lugar.

NICK SHOREY: Yo soy parte del equipo del GAC en nombre del Reino Unido. Estoy en un subgrupo que se focaliza en las actividades del grupo de trabajo de seguridad pública. Antes de dedicarme a la gobernanza de Internet era investigador de ciberdelitos y también un consumidor de servicios de dominio y de servicios de privacidad y proxy. Tengo visto este tema desde muchos ángulos. En el Reino Unido, como en muchos otros países, tenemos una amplia variedad de organismos gubernamentales responsables e interesados en la seguridad pública que se extiende a Internet.

En respuesta al lanzamiento del PSWG, es decir, el grupo de trabajo de seguridad pública, aunamos a todos los

departamentos para que pudiéramos hacer una consulta sobre todos estos temas. La parte de rentas o ingresos fiscales, aduanas, la oficina también de propiedad de la información, el organismo regulador de productos medicinales, otro organismo nacional dedicado a la lucha contra el delito, la policía del Reino Unido y también quienes integran la coalición de sociedades benéficas a favor de los niños por la seguridad de Internet. Tengo a John Carr aquí a mi derecha. Es representante de esa coalición.

Esperamos poder responder a esta pregunta que hizo David sobre el tipo de alcance amplio que tenemos en el grupo de trabajo de seguridad pública cuando pensamos en quiénes participan en él. Creo que en esta área, los gobiernos plantean sus preocupaciones y los problemas de manera muy clara. Hay mucha gente trabajando con este problema y tratando de entablar una interacción con la comunidad de Internet. A menudo estos profesionales, estas personas, han encontrado soluciones prácticas al problema.

Aquí a la izquierda tenemos a Jon Flaherty, investigador técnico y experto que va a contarles parte del trabajo que ha estado haciendo en el grupo de la especificación 11. Hemos realizado también reuniones mensuales en Londres hablando del trabajo y desarrollando recomendaciones consensuadas que luego forman parte de la respuesta del Reino Unido al PSWG pero

también es una manera maravillosa de compartir experiencia y discutir las mejores prácticas desde nuestra parte como gobiernos, para ver cómo podemos trabajar de manera más eficaz con la comunidad de Internet para tratar de dar solución a estos temas.

Como Fadi mencionó esta mañana, la ICANN es una parte del ecosistema de Internet y, en nuestro trabajo sobre gobernanza de Internet, nosotros vemos que este es un elemento de una estrategia más amplia y participamos en el foro de gobernanza de Internet. Ese es un muy buen ejemplo al igual que en el Consejo de Europa.

WANAWIT AHKUPUTRA: Nos quedan dos minutos, Nick.

NICK SHOREY: Muy bien, entonces tengo que apurarme. Vemos esto como parte de una estrategia más amplia. Ahora estamos tratando de desarrollar talleres de toda una jornada y quisiéramos que los registradores, las compañías que se ocupan de analizar las amenazas, que también contribuyan a eso.

Nosotros esperamos que este grupo pueda facilitar la colaboración y la participación activa entre el gobierno y la comunidad que conforma la ICANN para desarrollar soluciones

mutuamente beneficiosas y prácticas. ¿Cómo pueden participar ustedes? Si ustedes son miembros de un órgano de seguridad pública del gobierno pueden trabajar junto con su representante gubernamental que esté presente aquí en la ICANN. El grupo del Reino Unido también puede facilitar el contacto con otros miembros del GAC para llegar a las organizaciones de seguridad pública que corresponda. A veces es difícil encontrar a la persona adecuada así que acérquense a nosotros. Tal vez necesiten un punto de contacto del G7 o a alguien de la lista de preservación de datos del Consejo de Europa.

Si ustedes pertenecen a una comunidad más amplia pueden trabajar de manera directa o a través de los procesos de la ICANN y pueden colaborar para lograr estas soluciones prácticas mutuamente beneficiosas. Creo que cubrí todo lo que quería decir.

WANAWIT AHKUPUTRA: Jon, realmente nos quedamos sin tiempo así que les pido disculpas pero tenemos uno o dos minutos nada más para su intervención. Adelante, Jon.

JON FLAHERTY: Bueno, ¿cuán rápido puedo hablar? La especificación 11 ya es algo que ha sido mencionado aquí. Se ocupa de las cuestiones de uso indebido, de abuso, en torno al uso de los nombres de dominio. Surgió en respuesta al asesoramiento del GAC y del NGPC a partir de la reunión en Pekín. Les puedo dar una actualización rápida. Les puedo explicar el avance que hemos logrado en el grupo de trabajo. Esto es lo que vamos a discutir esta semana en la reunión 54 de la ICANN.

En cuanto a una relación entre el grupo de trabajo de seguridad pública y los registros, a mí me pidieron ser copresidente en este grupo de trabajo del marco de seguridad y yo dije: "Bueno, yo estuve trabajando en la investigación de ciberdelitos en el Reino Unido y nunca se pidió información en estos casos y nunca logramos una solución". A veces un registro tiene una innovación muy técnica que también raya en lo maravilloso. Entonces, en esta relación actual que estamos estableciendo con los registros, no esperamos que todos los registros sean capaces de darnos una respuesta pero sí que nos ayuden. Todavía no hemos armado por escrito el marco sobre el cual trabajamos sino que lo hemos simplemente puesto en la práctica.

¿Qué reseña general les puedo dar? Nos focalizamos en el uso y en las salvaguardas de los nuevos gTLD y la protección de los nuevos gTLD. También respondemos a las amenazas de

seguridad que llegan a través del software malicioso: los botnets, el phishing, la suplantación de identidad. El grupo está también viendo cómo un registro elige responder a las amenazas de seguridad porque queremos aportar en la sesión que tendremos con los registros y los registradores el miércoles, algunos estudios de caso para ver qué es lo que se está haciendo y cómo podemos continuar desarrollando una relación productiva.

El grupo de trabajo está conformado por profesionales, gente del ámbito del cumplimiento, de órganos de policía, de registros y registradores, del grupo de trabajo del GAC y ahora tenemos una voz y tenemos también un lugar en la mesa y tratamos de incidir en este marco. El beneficio mutuo es que todas las partes pueden profundizar en su conocimiento de las amenazas y reducir los tiempos para poder llegar a quienes utilizan botnets y software malicioso y phishing y ocasionan daños.

Estamos desarrollando un marco de seguridad central. Queremos definir la forma. Estamos trabajando en los principios orientadores pero no queremos ser demasiado restrictivos. Queremos ser muy flexibles sobre todo desde el punto de vista técnico cuando decimos que hay algunos registros que ya están trabajando, ya nos están dando este tipo de información con respecto a cómo responden a los abusos. También desarrollamos principios rectores de la ICANN en este proceso y

ya tenemos disponible una carta orgánica. No hay una política que funciona para todos los registros, para un registro puede funciona y para otros no, para proteger a sus clientes.

También queremos colaborar para poder intercambiar las mejores prácticas que existen hoy en día entre los distintos actores y, por último, queremos redactar un documento marco, establecer las pautas básicas y esperamos que para enero, para fines de enero del 2016 ya podamos tener un documento borrador que pueda ser sometido a comentario público. Muchas gracias.

WANAWIT AHKUPUTRA: Realmente nos quedamos sin tiempo pero le puedo dar la palabra a John Carr para que haga su presentación.

JOHN CARR: Puedo hacerlo en un par de oraciones. Obviamente nuestra coalición en favor del bienestar infantil está muy interesada en estos temas que se están discutiendo pero estamos trabajando activamente con la ICANN desde la creación de la última ronda de los nuevos gTLD y cuando se hizo la solicitud para .kids y otros nombres similares. Creo que es obvio decir que si vamos a crear un espacio que va a llevar en última instancia a la creación de sitios web que tienen la intención de atraer a grandes

cantidades de niños y de jóvenes, entonces nos parece que esto plantea preocupaciones desde el punto de vista de la seguridad y que tenemos que tener en cuenta desde el principio del proceso.

Cuando se hizo la última ronda, esto no fue así y queremos asegurarnos de que esto no vuelva a repetirse en el futuro. Por eso estoy tan complacido de ser parte de este proceso del grupo de trabajo de seguridad pública.

WANAWIT AHKUPUTRA: Muchas gracias a todos los oradores. Les pido disculpas porque realmente nos quedamos sin tiempo y vamos a revisar las preguntas que plantearon en las transcripciones y vamos a publicar las respuestas en nuestro sitio web.

ALICE MUNYUA: No vamos a responder una pregunta ahora pero vamos a pedirle que igualmente la plantee.

WENDY SELTZER: Muchas gracias. Quería brevemente referirme al tema de la seguridad pública. Como signataria de uno de los comentarios en este proceso de registración de servicios de proxy y privacidad, un comentario que fue elaborado por varias mujeres

defensoras de la inclusión de las mujeres afectadas y víctimas y sobrevivientes de abusos, y signatarios también de ese tipo de comentarios en los que se habla de la información privada que se publica en línea. Nosotros pedimos la protección de la información privada cuando redactamos esos comentarios y muchos tuvimos que ponernos en contacto con los organismos de aplicación de la ley para que supieran que se había publicado esta información en Internet.

Es como un proceso circular el que tenemos y a muchos de nosotros nos recuerda cómo a veces hay publicación forzada de información, muy similar a lo que solicita el WHOIS y en realidad esto constituye una invasión a la privacidad y también una preocupación desde el punto de vista de la seguridad pública y privada.

ALICE MUNYUA: Quiero aprovechar para agradecerle a todos los panelistas y a todo el público que participó. Claramente para la próxima sesión vamos a necesitar tres horas, no una hora y media. Trataremos de armar otra sesión para la próxima reunión de la ICANN. Muchas gracias a todos.

[FIN DE LA TRANSCRIPCIÓN]