KOBE – Segundo taller sobre políticas de los líderes de At-Large: equilibrar la privacidad con la seguridad y estabilidad para los usuarios finales de internet
Domingo, 10 de marzo de 2019 – 10:30 a 12:00 JST
ICANN64 | Kobe, Japón

YESIM NAZLAR: Hola. Bienvenidos a nuestra segunda sesión. Mi nombre es Yesim Nazlar. Antes de comenzar, quiero hacer un recordatorio, como ya es habitual. Como saben, contamos con interpretación en inglés, español y francés para la sesión del día de hoy. Así que, por favor, recuerden mencionar sus nombres en el momento de tomar la palabra y también, por favor, no olviden hablar a una velocidad razonable para poder ayudar a nuestros intérpretes. Y si quieren tomar la palabra, pueden colocar sus tarjetas identificativas en esta posición sobre la mesa. Eso es todo lo que tengo para comentarlos de momento. Ahora quiero darle la palabra a Jonathan. Gracias.

JONATHAN ZUCK: Gracias, Yesim, y gracias nuevamente a todos por estar presentes. Sé que las conversaciones fueron productivas. Con respecto a la última sesión que tuvimos, Glenn McKnight circuló un documento de Google Docs para que lo puedan verificar. Gisella

también lo va a circular en el grupo, simplemente para que ustedes puedan tener esta área comunitaria para compartir las notas y si hay alguna idea o comentario que quieran plasmar, lo pueden hacer allí. Lo vamos a hacer para ambas sesiones, así que gracias, Glenn.

Esta sesión nuevamente tiene como objetivo ser un debate interno de At-Large respecto de lo que quisiéramos lograr con respecto a los próximos pasos en relación al GDPR. Tenemos algunos invitados que son expertos en esta materia que nos han dado información. Y ahora lo que vamos a hacer es avanzar con el debate y hacer un seguimiento más de cerca. Quiero entonces continuar con el debate para que todos estemos en la misma sintonía.

También, como sucedió en la última sesión, tratemos de hacer lo posible para trabajar y avanzar en materia del EPDP en la fase uno.

El desafío de At-Large, uno de los tantos, y ya lo hemos debatido anteriormente, es que nosotros queremos trabajar en pos de los "usuarios finales". Por eso tenemos usuarios finales que son registratarios y no registratarios. Y hay más usuarios finales que no son registratarios. Entonces, estos intereses no necesariamente están en línea, y es allí donde nosotros tenemos que centrar nuestro debate en este tema.

También los usuarios no registratarios de cierta forma están poco representados en el debate. Y nosotros tratamos de ser la voz de esos usuarios no registrados para que sí puedan ser escuchados o tener una participación en el debate. No estamos diciendo de ninguna manera que los usuarios finales que son registratarios no tienen importancia, pero para este ejercicio entonces, si es posible, lo que vamos a hacer es lo siguiente. Vamos a debatir el tema desde la perspectiva de los usuarios finales que no son registrantes. Y eso es lo que queremos hacer. Y dado que nosotros tomamos esta decisión de avalar a estas personas, así vamos a llevar adelante el debate.

La cuestión de estos usuarios finales que no son registratarios también, de alguna manera, incluye a los que son registratarios, porque cuando yo, por ejemplo, voy a comprar un nombre de dominio, soy un registratario. Pero si voy a hacer una reserva para un ticket aéreo, entonces ahí estoy funcionando como un usuario no registratario. Entonces, creo que tenemos que abordar a los usuarios finales no como un grupo de personas que no son importantes, sino que tenemos que tener en cuenta que la mayor parte de nosotros trabajamos o hacemos actividades dentro de Internet, incluso mi hija Donna muchas veces trabaja en cuestiones de usuarios finales. Lo hacemos, por ejemplo, cuando

hacemos actividades de banca *online*, cuando participamos en grupos de trabajo, compras *online*, etc.

Es decir, hay actividades de los usuarios finales y todos somos usuarios finales. Pasamos a la siguiente diapositiva.

Entonces, en el camino hacia adelante, sabemos que la fase 1 está finalizada. Probablemente alguno me vaya a corregir, pero cuenten hasta diez antes de corregirme, por favor, porque la fase 1 está finalizada.

Básicamente lo que decidimos fueron las razones válidas para recabar datos, qué datos van a ser públicos y qué datos van a permanecer privados, dónde se aplica el GDPR. Esto es algo que estuvimos debatiendo. Y también a quién se aplica el GDPR. Sé que existen todavía algunos debates que están en curso. Y conforme pasemos a la fase dos, vamos a tener que hablar de quién va a tener acceso a los datos que se determinaron como privados y en qué circunstancias van a obtener ese acceso y mediante qué mecanismos van a acceder.

Básicamente este es el debate que vamos a tener. Estos son los puntos principales y es lo que vamos a debatir. No sé si alguno quiere hacer algún cambio al respecto. Bien, veo que no, así que entonces pasamos a la siguiente diapositiva.

¿Quién querría tener acceso a los datos? Bueno, tenemos a las agencias de cumplimiento de la ley para cuestiones de protección del consumidor, investigadores en materia de ciberseguridad para cuestiones de seguridad y estabilidad, sistemas que tienen que ver con la reputación, por ejemplo, para prevenir el *spam*, el *malware*, *phishing*, y también los titulares de propiedad intelectual para sus propios intereses, pero esto tiene algunas implicancias o consecuencias en materia de protección al consumidor. Como se dijo anteriormente, también hay algunas consecuencias en materia de *malware*, fraude y falsificación. Esto también es parte de los temas que se van a debatir. Siguiente diapositiva, por favor.

Bueno, la discusión que quiero tener ahora tiene que ver con el cumplimiento de la ley. Algunas de las preguntas a tener en cuenta para debatir son las siguientes. ¿Cómo las agencias de cumplimiento de la ley utilizan los datos actualmente? ¿Hay otras formas de obtener datos más allá de los registros de registración? ¿El cumplimiento de la ley automáticamente está abarcado dentro del GDPR? Y si no es así, ¿qué es lo que hay que tener en cuenta? Y, finalmente, cómo el cierre efectivo del WHOIS afectó a las agencias de cumplimiento de la ley en el último año. Aquí vamos a ver algunos ejemplos de lo que ha sucedido. Quizás

alguien tenga alguna anécdota que quiera compartir con nosotros con respecto a estos puntos.

Entonces, lo que voy a hace es comenzar con Laureen para que nos cuente su perspectiva sobre estas preguntas. Y después les voy a dar la palabra a ustedes para que efectúen sus comentarios al respecto. Esto, como dije anteriormente, es un debate y no hay nadie que tenga que ganar en este debate. La idea es poder tener más información.

Laureen, adelante, por favor. La idea como dije es plantear la información, seguir continuando con los debates, determinar de qué manera vamos a enfocar la fase dos y no solamente reiterar información del proceso anterior. Así que Laureen tiene la palabra.

LAUREEN KAPIN: Gracias. Soy Laureen y les doy las gracias por la oportunidad de hablar y de abordar estas preguntas más importantes. Yo soy abogada de la Comisión Federal del Comercio de Estados Unidos. Trabajo con varias agencias del cumplimiento de la ley en Estados Unidos. Son agencias que abordan el tema de la protección y la confianza de los consumidores. Así que básicamente esto es dentro de la Comisión de Comercio.

También tenemos un foco en la competencia, pero yo particularmente no me ocupo de ese tema.

Por supuesto, no voy a querer ganar hoy, pero sí me gustaría compartir con ustedes algunas perspectivas con respecto a por qué es importante el WHOIS para las autoridades de cumplimiento de la ley que se abocan a la competencia de la protección del consumidor. Yo agradezco el enfoque que la comunidad de At-Large que coloca en los usuarios finales que no son registratarios. Esto de tener a alguien que hable por los usuarios finales. Entonces quiero tomar en cuenta lo que dijo Jonathan con respecto a que los usuarios finales muchas veces están poco representados en este tipo de debates. Los usuarios finales, por supuesto sí son parte del mandato clave de la Comisión Federal de Comercio porque muchas veces están sujetos o son víctimas de usos indebidos o malas prácticas dentro de Internet.

Habiendo dicho esto, quisiera hablar sobre cómo las agencias de cumplimiento de la ley confían en el WHOIS. Probablemente esto ya lo han escuchado antes, así que no voy a entrar en detalles.

Básicamente, nuestra agencia utiliza el WHOIS como una herramienta de investigación, y lo utilizamos como herramienta de investigación para todo, por ejemplo, para las cuestiones que tienen que ver con la refinanciación de hipotecas, para

determinar la gente que quiere tener ciertas oportunidades con respecto a los créditos, para créditos con menores tasas, para identificar estafas, también para identificar sitios web o correos electrónicos. El WHOIS fue uno de los lugares principales que tuvimos en cuenta para determinar quién está detrás de, por ejemplo, un nombre de dominio o sitio web que trata de obtener datos de determinados consumidores.

También recurrimos al WHOIS cuando existen ciertas cuestiones que tienen que ver con la privacidad y la violación de la privacidad, por ejemplo, cuando hay *malware* o *spyware* que se instala en el sitio web de un usuario. Así que en ese caso lo que hacemos es recurrir al WHOIS para determinar cuáles son los atributos, quién está detrás de un ataque de *phishing* o de una instalación de *spyware* que infringe o que perturba la privacidad de un usuario. Básicamente utilizamos nuestro mandato jurisdiccional para poder proteger estas cuestiones. No solamente nos ocupamos de las actividades de fraude o actividades engañosas, sino también de infracciones de la privacidad.

No somos la única agencia de cumplimiento de la ley en el mundo y en los Estados Unidos que usa el WHOIS. Supongo que mis colegas que también trabajan activamente en el Grupo de Trabajo de Seguridad Pública – esa es otra de las funciones que

tengo yo. Soy copresidente de este comité de trabajo dentro del Comité Asesor Gubernamental.

Tenemos también representantes del Servicio Secreto de Estados Unidos. Ellos tienen un mandato bastante amplio, más allá de proteger al presidente y más allá de lo que vemos en las películas. Pero también brindan seguridad en varios aspectos, como por ejemplo en eventos públicos donde hay figuras públicas que pueden aparecer. Entonces, básicamente a veces hay amenazas que ellos detectan para esos eventos y que tienen conexión con sitios web. Y para eso utilizan el WHOIS, para poder encauzar las investigaciones.

Es el WHOIS el que los ayuda a identificar patrones de actividad. Por ejemplo, si hay un nombre de dominio que está interesado en utilizar herramientas de un tercero, lo que van a hacer es ver quién es el titular de ese nombre de dominio o si, por ejemplo, es Pedro X, y van a investigar quién es esta persona.

Cuando hay amenazas en ciertos eventos también, por ejemplo. O para ciertas personas. También cuando hay cuestiones de contrabando o actividades de contrabando utilizan el WHOIS como una herramienta de investigación.

Y podría contarles un montón de cuestiones al respecto que tienen que ver con los correos electrónicos que están

comprometidos, también gente que utiliza grandes cantidades de dinero. Esto obviamente da lugar a grandes fraudes en todas partes del mundo, como los fraudes de romance. Es decir, hay muchas actividades de las cuales se ocupa el Servicio Secreto de los Estados Unidos.

También el Departamento de Comercio de los Estados Unidos se centra en la ciberseguridad, porque esto está incluido dentro del mandato y esto incluye la protección de los niños, la protección y seguridad de los nombres de dominio. Y es el WHOIS el que permite rastrear los nombres de dominio que están asociados con estas actividades fraudulentas.

Lo que voy a decir es que hay muchas actividades en las cuales se puede utilizar el WHOIS para evitar que sucedan estas actividades maliciosas. Por lo tanto, el WHOIS es una herramienta muy importante.

Jonathan no me puso un límite de tiempo para hablar, lamentablemente, así que yo me estoy extendiendo.

Con respecto a otras formas de obtener los datos más allá de los registros de registración, bueno, sí, existen otras formas como ciertas órdenes de notificación. Son herramientas importantes, pero llevan mucho tiempo porque implican recurrir a un tribunal para que el tribunal emita cierta aprobación. Y esto es algo que

lleva más tiempo y requiere de más recursos que buscar un nombre en una base de datos que se hace en cuestión de segundos. Hay alternativas, por supuesto, pero requieren de mucho más tiempo y de muchos más recursos, lo cual significa que hay menos trabajo de investigación y cuando son emergencias críticas, no es factible estar en una posición en la cual hay que esperar para obtener estos datos. Es decir, no podemos esperar a que se apruebe una cédula de notificación o una orden judicial y que la apruebe un tribunal.

La última pregunta, y probablemente Greg pueda contarnos mucho más al respecto, pero sí quiero abordar la tercera pregunta, que es muy importante y es un tema principal, y es si el cumplimiento de la ley está automáticamente cubierto por el GDPR. Bueno, no, no es el caso. Esto no es así, especialmente para las agencias de cumplimiento de la ley extranjeras.

El GDPR reconoce plenamente un equilibrio que se tiene lograr entre la protección de la privacidad de los usuarios y la necesidad que tienen ciertas entidades de acceder a la información. Pero resulta bastante inquietante que el término de autoridad pública según el GDPR no ha sido interpretado tal como se entiende y, por lo tanto, no incluye a las autoridades de cumplimiento de la ley extranjeras, es decir, que no están dentro de la Unión Europea.

Si uno no está dentro de la Unión Europea, no está cubierto por el GDPR y probablemente necesite justificación para poder obtener esta información. Pero no queda para nada claro si esto es igual para todos.

El GDPR es muy extenso, es muy complicado y aun así tiene que seguir siendo interpretado por las entidades judiciales dentro de la Unión Europea, así que existe cierta flexibilidad, pero hasta el momento, según entiendo, no hay ningún camino concreto o claro para que las agencias de cumplimiento de la ley puedan obtener información según el GDPR. Y esto es un problema serio, en particular para alguien que proviene de los Estados Unidos, es decir, para alguien como yo que viene de una agencia de cumplimiento de la ley extranjera.

Entonces, cómo las agencias de cumplimiento de la ley utilizan el WHOIS es algo importante y si esto nos va a permitir continuar trabajando, bueno, esto es algo realmente crítico. Y es un área que tiene varios blancos o varias barreras desde la perspectiva del GDPR para las agencias de cumplimiento de la ley en el mundo.

JONATHAN ZUCK: Gracias, Laureen. Quiero dar la palabra a Kathy y a Farzi. Ustedes van a determinar quién va a hablar de cada tema. Pero creo que

Kathy dijo que la cantidad de actores maliciosos es poca en relación a otros. Pero también se mencionó que los derechos muchas veces implican intereses, así que la desventaja de revelar datos es que a veces tiene consecuencias. Pero bueno, sí, uno también tiene que hablar de qué piensa de las agencias de cumplimiento de la ley en este sentido y es lo que se está haciendo.

KATHY KLEIMAN: Gracias, Jonathan. Yo les quiero contar un poco al respecto antes de abordar de lleno la pregunta.

Soy Kathy Kleiman, soy cofundadora de la Unidad Constitutiva No Comercial y ya he participado en otras reuniones. Desde hace tiempo participo en este tipo de reuniones.

Voy a hablar más lento.

Hablemos un poco de la historia. Si Internet fuese simplemente comercio electrónico, sería una cuestión. Pero en realidad Internet es un canal de comunicación sumamente importante, el mayor de la humanidad. Entonces, hace años, cuando esto estaba dentro de los Estados Unidos, había una especie de regla que para poder imprimir algo había que brindar un nombre, una identificación y tener una autorización del gobierno. Y esto era criticado. Nosotros nos opusimos a eso y para eso tuvimos la

primera enmienda. La idea no era proteger a la prensa escrito, sino proteger a los usuarios finales, a las personas que iban a obtener ese tipo de comunicación. Queríamos saber qué era lo que sucedía, porque había muchos ciudadanos de muchos países cuestionando lo que hacían los gobiernos.

Hace unos años representé al grupo de trabajo de derechos humanos, que publicaba información sobre corrupción de sus propios países. Los nombres de dominio hablaban de la venta de recursos públicos a gente privada que formaban parte de la familia del presidente. Entonces había mucha corrupción que iba a ser tenida en cuenta también por los observadores de las elecciones.

Entonces había mucha información que brindaban los nombres de dominio y había muchos sitios web, pero era el único lugar donde se podía obtener información real porque en realidad los miedos de comunicación estaban a la orden del gobierno y también se nos dijo que si eso seguía así íbamos a ser arrestados. Y esto también tiene que ver con los servicios de privacidad y de representación.

A mí me preocupa mucho lo que dice el WHOIS o lo que está dentro del WHOIS. Y dijimos, “Tenemos un problema. La ICANN trabaja con las agencias de cumplimiento de la ley en los Estados Unidos”. Pero cuando aparece China o cuando alguien viene y me

dice, “Quiero información” o, “Quiero que haya una baja de determinado nombre porque hay una violación”, yo digo, “A ver, un momento. ¿Es una violación en China? ¿Y por qué se supone que hay que dar de baja un determinado nombre?”

Esto da lugar al problema del cumplimiento de la ley a nivel global. No todas las agencias de cumplimiento de la ley operan de la misma manera. Tenemos un proceso de debida diligencia y también tenemos acceso limitado, pero aun así existe un proceso y tenemos esta protección, y esta protección protege a los usuarios finales también.

Podría decir mucho más. Y si hay preguntas estoy dispuesta a responderlas. Pero GDPR da mucha más protección. La base de datos WHOIS fue creada antes de ICANN y antes de que existiéramos nosotros. Se creó cuando la red era una red de confianza, con personas de confianza. Y no hablaba de datos personales, era una cuestión de sistemas. Pero ahora las cosas se complicaron, es mucho más. Así que les dejo a ustedes la pregunta. Gracias.

JONATHAN ZUCK: Gracias, Kathy. Para dar un poco más de contexto a futuro, ya no tendremos un WHOIS público. Entonces, ¿hay soluciones para tener acceso a los datos que serían mejores que lo que tenemos

ahora? Porque la idea de ser público es para mantener la conversación en un tono de futuro.

KATHY KLEIMAN: Lo que oigo decir mucho, y lo tenía en mente pero no lo dije, es que las agencias de la ley quieren acceso ilimitado porque es cumplimiento de la ley. En Estados Unidos, las agencias de cumplimiento de la ley me lo dicen y también en el extranjero. Soy muy apasionada sobre este tema. Quieren que el WHOIS sea ilimitadamente público. Ellos quieren todo el acceso al WHOIS que necesitan. Y ese es el punto de partida de lo que estoy oyendo.

Entonces, ¿cómo conseguir el equilibrio? Incluso desde una agencia de la ley que somos, nosotros nos preguntamos, ¿cómo hacemos las preguntas correctas? ¿Qué es el debido proceso cuando hablamos de una organización como la ICANN de múltiples partes interesadas que hacen estas preguntas tan importantes?

JONATHAN ZUCK: Farzaneh, ¿quiere agregar algo? Preséntese, por favor.

FARZANEH BADII: Yo soy Farzaneh Badii, de la NCUC. Quería decir que la misión no es divulgar el trabajo, sin embargo, todas las agencias de cumplimiento de la ley del mundo deben rendir cuentas. Eso nosotros lo sabemos. Y deben existir medidas que permitan que ellas rindan cuentas si hacen un uso indebido del acceso a los datos.

Eso es muy importante para nosotros. Sin embargo, también oímos que el WHOIS se está usando para propósitos que no corresponden con la misión de la ICANN. Ahora bien, esto es muy controversial. Hay conflictos respecto de esta noción. Pero esa es mi idea.

Otra cosa que quería decir es, ¿por qué considerar que privacidad y seguridad se contraponen? No es así. Debe existir un equilibrio.

Si queremos trabajar en seguridad, tenemos que tener medidas implementadas que permitan dar a conocer los datos a los titulares de intereses legítimos y no al público en general. Lo que a mí me preocupa, y es una preocupación desde hace 20 años, es que ha habido un movimiento a que el WHOIS sea siempre público, es decir, no se procura alcanzar un equilibrio. Y los actores quieren que los datos del WHOIS sean públicos. Es el nombre, es el número telefónico del registratario, la dirección de correo electrónico.

Sería bueno si los actores reconocieran que la privacidad de los nombres de dominio de los registratarios es importante no solo para ellos sino también para los usuarios finales.

Por último, cuando hablamos del secuestro de nombres de dominio, su índice ha venido bajando desde que la base se ha tornado privada. O sea que no es que exista una falta de medidas. Tiene que haber un equilibrio entre las acciones malas que resultan de haber tornado WHOIS privado y las cosas buenas. Eso es todo. Tenía otra cosa que quería decir, pero me olvidé.

JONATHAN ZUCK: ¿Sobre el cumplimiento de la ley?

FARZANEH BADII: Sí.

El acceso por parte de las agencias de cumplimiento de la ley a los datos. Y usted, John, lo mencionó. Que los datos del WHOIS están expurgados en todas partes y que no tenemos que volver a discutir estas cuestiones. Hubo intentos en el EPDP de hacer una diferenciación geográfica al respecto. El GDPR no se aplica en estas regiones, por ejemplo, entonces estos registratarios de estos nombres de dominio, esos datos tienen que ser públicos.

Bueno, no, en realidad ese problema no lo hemos resuelto. Eso es todo.

JONATHAN ZUCK: Gracias, Farzaneh. ¿Alguien quiere comentar algo? Greg, ¿usted quiere agregar algo? ¿No? Bien. ¿Alguien tiene alguna pregunta? Ustedes han escuchado ambos lados de la historia en el contexto de la aplicación de la ley. No hemos entrado en otros contextos, pero quería saber si tienen alguna consulta sobre los actores.

Olivier.

OLIVIER CRÉPIN-LEBLOND: Muchas gracias, Jonathan. Quiero hacer una pregunta a Kathy, y probablemente me va a odiar por ello, por lo cual pido disculpas por adelantado.

En 2016, Kaspersky Labs registró 758 mil millones de ciberataques. ¿Cuántas personas fueron a la cárcel en relación con este hecho de que hicieran públicos los registros del WHOIS? Porque me imagino que no ha sido tanta gente.

KATHY KLEIMAN: Le permitiré contestar a Farzaneh.

FARZANEH BADII: Tengo una pregunta. ¿Qué es un ciberataque? Porque no todos son relacionados con el WHOIS. Hay matices. ¿Usted quiere saber cuántas personas han ido a prisión por el acceso al WHOIS? Sí, hay algunos, pero también hay cuestiones de acoso. Pero no datos son publicados. Los gobiernos no salen a decir, "Usé datos personales de registratarios en el WHOIS". No lo dicen, pero hay ejemplos y lo estamos documentando. No queremos decir que haya llegado el fin del mundo cuando los datos sean públicos, pero existe un riesgo.

OLIVIER CRÉPIN-LEBLOND: Si me permite agregar, es una buena respuesta. Yo no quería saber en general cuántos, pero es bueno para la sociedad civil hacer un rastreo.

FARZANEH BADII: Si una persona va a la cárcel por esta cuestión, tenemos que preocuparnos.

OLIVIER CRÉPIN-LEBLOND: Quizá deberíamos considerar el mismo enfoque con lo que es *spam* y *malware*.

JONATHAN ZUCK: Bueno, se está conversando sobre los estados involucrándose. Aquí las apuestas son más altas. Vale la pena esta conversación.

¿Dmitry primero? Andrei.

ANDREI KOLESNIKOV: No soy Dmitry. Soy Andrei.

JONATHAN ZUCK: Estaba haciendo un chiste.

ANDREI KOLESNIKOV: Quería pedirles a todos que se restrinjan al tema de la charla de hoy y que no hablen de mandar a la gente a la cárcel o sobre la violación de minorías o mayorías. Tenemos un tema y pido que todos nos ciñamos a este tema. Gracias.

KATHY KLEIMAN: Si me permite, la aplicación de la ley siempre está relacionada con los derechos del ciudadano. No entiendo por qué entonces no está relacionado con el tema. Aquí estamos para hablar de un equilibrio que se debe alcanzar.

ANDREI KOLESNIKOV: Quizá no fui claro. Hablo de los datos que tienen que ver con el cambio del GDPR, la especificación temporaria, etc. Esto está estrechamente relacionado con las actividades de la ICANN, y quizás estamos demasiado focalizados. Tenemos poco tiempo.

Tenemos a Greg. Tenemos a otros. ¿Por qué no nos centramos en el tema de los datos?

KATHY KLEIMAN: No tenemos esos datos.

JONATHAN ZUCK: Tratemos de confinar esto al tema rápidamente. Somos una comunidad muy amplia en At-Large y no todos tenemos la misma concepción sobre estos temas. Entonces, este ejercicio en parte es poner los hechos delante de las miras nuestras y ver si podemos llegar a un consenso más adelante. Tratemos de hacerlo así. ¿A quién tenemos? Ricardo.

RICARDO HOLMQUIST: Voy a hablar en español. Pido disculpas.

JONATHAN ZUCK: Por favor, adelante.

RICARDO HOLMQUIST: La pregunta que tenía era para la primera persona que habló, perdón, pero no veo el nombre. Creo que es Laura. Sí, Laureen, perdón.

La pregunta que tenía era si hay estadísticas de esa data que decía porque, al igual que en derechos humanos, tenemos un problema serio cuando los países, sobre todo cuando hablamos de países que no son totalmente democráticos, y pueden ver la data del WHOIS. En un país como el suyo lo puede hacer más democrático, pero, ¿cuántas veces necesitas entrar al WHOIS para revisar algo? ¿Una vez al día, una vez al mes? ¿Cien veces diarias? O sea, ¿hay estadísticas de cómo se está utilizando eso y cuánto afecta realmente a esto? Porque si es una vez al día, tener que ir a un juez a pedir una orden no parece ser un problema importante, sobre todo cuando en países como el mío se puede ir preso nada más porque no fue al juez, sino que directamente se abrió el WHOIS y metieron presa a la persona. O sea, tenemos que tener el balance, ¿no? Y por eso quería saber si había alguna estadística. Gracias.

LAUREEN KAPIN: Gracias por su pregunta. Estoy segura de que existen estadísticas. Pero no se las puedo brindar ahora, no las tengo. Sin embargo, puedo contarle, por lo que he venido hablando con mis colegas del mundo de la aplicación de la ley, que hay muchas agencias en Estados Unidos y el resto del mundo que utilizan el WHOIS al menos cientos de veces por día, quizá más, porque tienen un gran volumen de investigaciones y ese es el volumen del trabajo que

realizan. Otras agencias, por ejemplo la mía, quizá lo usen con menos frecuencia, pero hay un rango muy amplio de usos. Observo además que hay muchas agencias de aplicación de la ley que lo usan una vez por día si no tienen una carga de trabajo activa. Pero estoy haciendo generalizaciones. Algunas agencias llevan estadísticas, pero no se las puedo reportar en este momento. No obstante, me agrada ver que haya hecho esta pregunta porque me permite reconocer puntos muy válidos que hicieron mis amigos del otro lado la mesa, Kathy y Farzaneh, cuando dijeron que estas son cuestiones muy importantes en lo que tiene que ver con el uso indebido del WHOIS y cómo la gente puede estar en una situación de peligro. Me gustó el ejemplo de los primeros días de nuestro país porque es un ejemplo de la restricción.

No creo que ninguno de nosotros en la sala podamos respaldar que se use el WHOIS para hacer una restricción de la libertad de expresión. Hay que reconocer, no obstante, que existe un riesgo que tenemos que manejar. Entonces, cuando hablé de estos peligros financieros, riesgos físicos, todas estas instancias que están documentadas por estadísticas, *malware*, intrusión de redes, *phishing*, *farming*, todas esas cosas malas que permiten que se realicen estafas y permiten explotación infantil y otros delitos graves, bueno, hay un equilibrio que alcanzar y la

comunidad está intentando encontrar el punto de equilibrio justo. Estoy hablando desde la perspectiva de una agencia de la ley. Estoy en los Estados Unidos. Y a nosotros nos interesa proteger al público. Pero debo reconocer que mis colegas han hecho puntos muy válidos, que no todos los gobiernos tienen las mismas prioridades. Es una realidad que tenemos que aceptar.

JONATHAN ZUCK: Gracias, Laureen. Hay varias personas que quieren hablar. Si me permiten, entonces pongamos algunos parámetros.

Como tenemos estos panelistas, tomemos esta sesión como una sesión para determinar hechos. Tratemos de obtener la mayor cantidad de información de los panelistas posible, porque no usemos este tiempo para expresar nuestras opiniones. Es un recurso muy valioso. Yo pensé que esta discusión que iba a ser la más sencilla y ya viene una discusión muy nutrida.

Ahora, las preguntas que van a hacer son para obtener más claridad de los panelistas, no para debatir el tema, porque ese debate lo tendremos más adelante. Tratemos de hacer las preguntas más claramente. Humberto.

HUMBERTO CARRASCO: Muchas gracias. Voy a hablar en español. Voy a esperar un minuto porque mi pregunta va dirigida a Farzaneh y a Kathy.

Creo que Farzaneh mencionó que se discutió en algún momento la posibilidad de distinguir entre aplicar el GDPR de acuerdo a las regiones, que supuestamente era aplicable a la normativa y aquellas que no eran aplicables.

Entonces aquí hay un problema de lo que se conoce como extraterritorialidad de la ley. Yo soy chileno, sudamericano. Muchos de los abogados de mi país decían, bueno, esto aquí no se aplica, nosotros no tenemos nada que ver con Europa. Pero, por ejemplo, tenemos el caso de Ricardo Holmquist, que tiene doble nacionalidad. Él es venezolano e italiano. Entonces, este hombre estaría protegido por la GDPR aun cuando vive en Venezuela.

Entonces, ¿cuál es el problema que tenemos ahí? El problema es que nosotros vamos a tener que respetar la GDPR en el caso que tratemos los datos de Ricardo porque él tiene doble nacionalidad. Pero, ¿cómo ustedes van a poder, aquellos que manejan los datos, distinguir qué persona tiene o no doble nacionalidad? Ese es un problema y por eso tengo esta pregunta. ¿Cuál sería la solución ahí?

JONATHAN ZUCK: Tengo la certeza de que nadie tiene la respuesta a esa pregunta.

FARZANEH BADII: GDPR no tiene que ver con nacionalidades. GDPR solo se ocupa de la existencia física del sujeto de datos dentro del área económica europea. Entonces, si usted es un ciudadano no europeo y reside en el área económica europea, entonces el GDPR se le aplica. Pero para ciudadanos europeos que no residen en regiones en el área económica europea, el GDPR no aplica. Entonces no tiene que ver con ciudadanía. Y si hubiera tenido que ver, habría sido muy difícil. Se hubiera necesitado recolectar pasaportes. Sería imposible tener los pasaportes de todos. Gracias.

JONATHAN ZUCK: Marita.

MARITA MOLL: Gracias. Mi pregunta es para Laureen. Usted dijo que una de las barreras del WHOIS es que lleva mucho tiempo conseguir la información en caso de violación. En algunas sociedades democráticas es una concesión que normalmente hacemos a los abogados si queremos hacer escuchas telefónicas o vigilancia de domicilios.

Ahora, como es la Internet y todo va tan rápido, ahora tenemos que tenerlo instantáneamente. Ya no tenemos ese tiempo que necesitamos para hacer ese trabajo de contexto, de fondo, que es esa concesión que siempre hemos hecho entre privacidad y seguridad.

¿Hay una evidencia aquí que indica que esto sea una característica negativa?

LAUREEN KAPIN: Un par de respuestas breves. En primer lugar, no estamos abogando por retornar al WHOIS público. Reconocemos que el GDPR ya es una realidad. Entonces, parte de la premisa de su pregunta parece implicar que nosotros decimos que quisiéramos volver a como eran antes las cosas, y eso no es exacto. Y no es eso lo que nosotros estamos defendiendo. Primer comentario.

En segundo lugar, sí, hay evidencia de que las investigaciones si no llevan el tiempo adecuado hay perjuicios. Greg va a hablar más al respecto.

Con respecto a la pregunta filosófica, y me gustan las preguntas filosóficas, nosotros también vivimos en un mundo donde tanto usted como yo, que tenemos información sensible en la Internet, tenemos el derecho a saber con quién estamos tratando. Tenemos guías telefónicas, directorios comerciales, muchas

situaciones. No es una escucha telefónica, es contacto. Es información de contacto, no contenido. Las informaciones de contacto las necesitamos para el trabajo. El público tiene que tener acceso a esta información para poder operar con seguridad y saber con quién está haciendo negocios. Y además, en el área de cumplimiento de la ley tenemos otras responsabilidades superiores. He intentado de alguna manera cubrir la base de su pregunta.

JONATHAN ZUCK: Tenemos a Alan ahora.

ALAN GREENBERG: Muchas gracias. Dos comentarios. Hadia se refirió un poco a lo que dijo Humberto. Pero la respuesta es más compleja. Hay quienes en Chile serán sujetos del GDPR. No por su ciudadanía necesariamente, sino por su empresa. Es una cuestión compleja. No es simple.

Con respecto a las estadísticas, el Equipo de Revisión del WHOIS va a publicar su informe en pocas horas e hizo un relevamiento de lo que es la aplicación de la ley en el mundo. Lo que aparece en el informe final no es muy distinto de lo que había en el borrador. Y ahí hay bastantes estadísticas de frecuencia de uso del WHOIS, del impacto que significaría no tenerlo. Hicimos un

relevamiento unos pocos meses después de que saliera la especificación temporaria, así que hay una muestra. Son números duros, es un relevamiento preliminar. Todavía no hay evaluación, pero están empezando a surgir las cifras.

HOLLY RAICHE: A mí me gustaría escuchar de ambas partes lo siguiente. Se ha aceptado en los Estados Unidos y en los países occidentales que existen cuestiones a favor y en contra y se está reconociendo este equilibrio que debe existir para la obtención de información por parte de las agencias de cumplimiento de la ley que no siempre se puede medir. Entonces, si dejamos esto de lado, ¿qué tipo de prueba ustedes podrían tener en cuenta para la especificación temporal? Para decir que vamos a permitir que esas agencias de cumplimiento de la ley que sí respetan la privacidad de los usuarios puedan acceder a estos datos, en comparación a aquellas otras que no respetan la privacidad. Me parece que no vamos a lograr un acuerdo en esto. Probablemente Kathy y usted me puedan responder, pero, ¿qué pasa con esas personas en países con leyes que no los protegen?

LAUREEN KAPIN: Parece que nadie quiere tomar la palabra, así que voy a hablar yo. Es una pregunta muy difícil de responder realmente. Y no tengo

la respuesta. Tampoco sé si existe una respuesta sencilla y concreta al respecto. Me gustaría poder decir que sí tengo esa respuesta, pero sé que el trabajo del área dos se va a centrar básicamente en esto. Como dijo Jonathan anteriormente, quién necesita el acceso, para qué, qué procedimientos se van a seguir para lograr ese acceso. Entonces estos son los puntos que se van a tener que tomar en cuenta para responder a la pregunta. Pero sí, es una cuestión muy, muy complicada.

KATHY KLEIMAN: Yo le estaba preguntando a Farzi qué está sucediendo ahora en el EPDP con respecto a este tema, porque no lo sabía. Pero yo creo que habrá que determinar cierta jurisdicción. Incluso si uno no está conforme o contento con esto. Como dije antes, yo soy abogada dentro de los Estados Unidos.

La idea de tener un registro, un registratario, un registrador y que puedan existir en un país con libre expresión y que los datos del registratario puedan ser requeridos por una agencia de cumplimiento de la ley en una región totalmente distinta del mundo, bueno, probablemente esto implique diferentes cuestiones para los países. Y esto es lo que va a abordar la fase que sigue, es decir, quizás analizar esta relación entre las agencias de cumplimiento de la ley y la jurisdicción que tiene el registro, el registrador y el registratario.

LAUREEN KAPIN: Voy a dar una breve respuesta al respecto. La inquietud que yo tengo con ese enfoque es que en cuanto a las estafas y los fraudes y este tipo de actividades que se llevan a cabo en el mundo, no están solamente en una única jurisdicción. Las investigaciones de las agencias de cumplimiento de la ley, como ustedes saben, muy a menudo en la actualidad se llevan a cabo en jurisdicciones diferentes, en múltiples jurisdicciones. Entonces, tener esto que esté basado en la jurisdicción, probablemente solamente la gente de los Estados Unidos pueda obtener información sobre la jurisdicción de los Estados Unidos. Yo entiendo lo que usted quiere decir con respecto a qué sucede si una agencia de cumplimiento de la ley quiere obtener información sobre un registratario en China. Pero esto no toma en cuenta los fraudes o este tipo de actividades que las agencias de cumplimiento de la ley tienen que investigar y que muy a menudo tienen lugar en la escena internacional.

KATHY KLEIMAN: Bueno, la respuesta serían las agencias de cumplimiento de la ley internacionales. La ICANN como organización debe reconocer que se opera a un nivel internacional. Pero las agencias de cumplimiento de la ley también operan dentro de las leyes locales. Entonces muchas veces se determina que una agencia de

cumplimiento de la ley no puede existir en otro país. Ya debatimos esto.

Pero sabemos que los fraudes y las estafas muchas veces vienen de un determinado país. Hay gente que se va de esos países por cuestiones de genocidio, por ejemplo. Y hay también países que están dedicados a la eliminación de determinados grupos en un determinado país. Entonces es importante que los países puedan investigar al respecto.

Y es importante decir que el GDPR no solamente protege a las personas, sino que también protege a los territorios, la identidad sexual, cuestiones políticas o de género. Es decir, hay una serie de organizaciones no comerciales que también están abordando este tema de la protección que se da dentro del GDPR, independientemente de que las agencias de cumplimiento de la ley no sepan de qué organizaciones se trata.

JONATHAN ZUCK: Tiene la palabra Hadia.

HADIA ELMINIAWI: Yo tengo una pregunta. Creo que no respondimos de qué manera esta restricción efectiva del WHOIS afectó a las agencias de cumplimiento de la ley. Probablemente tengamos que comentar

al respecto. Pero tengo una serie de puntos que mencionar. En realidad, hay comunidades vulnerables y es muy importante protegerlas. Ya existen muchos mecanismos mediante los cuales uno puede proteger estas comunidades vulnerables. Estas cuestiones como la privacidad de la representación, quizá no bajo este punto, pero sí hay medios mediante las cuales las comunidades vulnerables pueden ser protegidas.

Por otro lado, tenemos que tener en cuenta también que hay ciudadanos que están sujetos a la explotación infantil, a la trata de blancas, etc. Y estas no son cuestiones únicas.

Y un último punto. Todos estamos de acuerdo, y no es volver a lo que se dijo anteriormente – pero lo que estamos debatiendo aquí es el acceso de las agencias de cumplimiento de la ley a través de un mecanismo para poder acceder a los datos no públicos. Todavía no hemos debatido nada que sea realmente concreto en ese sentido, pero obviamente, mediante este tipo de mecanismos se va a poder saber quién accede a los datos, qué agencia de cumplimiento de la ley tiene acceso a los datos.

En caso de que exista alguna violación a alguna clase de derecho del ciudadano, se debe poder poner la responsabilidad en aquellas personas que realmente son responsables de eso.

Una vez más, estamos hablando de un sistema totalmente diferente en el cual las comunidades vulnerables van a poder ser protegidas y, como dije anteriormente, ya hay mecanismos implementados para poder lograrlo.

Ahora bien, con respecto al tema de la jurisdicción y esta cuestión de las agencias de cumplimiento de la ley y la jurisdicción, debo decir que yo vengo de un contexto técnico, pues soy ingeniera en comunicaciones, con lo cual tengo muy poco conocimiento legal. Pero en algunos casos me parece que uno realmente no conoce la jurisdicción del sitio web con antelación o antes de obtener información de ese sitio web.

Entonces, esta suposición de que uno sabe o conoce la jurisdicción con antelación a dar el primer paso, me parece que no es del todo real. Gracias.

JONATHAN ZUCK: Gracias, Hadia. Voy a cerrar la lista de oradores, pero quiero reiterar que aquí no estamos tratando cambiar el punto de vista de nadie. Simplemente estamos tratando de informarnos entre nosotros de la mejor manera posible. Así que les pido que tengan esto en cuenta. No queremos convencer a nadie. Y no quiero que se arme un debate de todo. Hay que seguir avanzando con el tema. Bien.

KATHY KLEIMAN: Yo debo decir que no estoy de acuerdo, Hadia. Usted está en el EDPD y hace un seguimiento muy de cerca de este tema y yo también estoy haciendo un seguimiento muy cercano de todos los temas. Y esto también está en el EPDP, así que la transparencia en sí no es suficiente, sino que es un mecanismo que se da por sentado.

En los Estados Unidos, nosotros tuvimos un problema con las salas de chat porque la gente utilizaba nombres distintos y muchas veces se venía y se preguntaba, “Nosotros queremos saber cuál es la identidad de esa persona porque está cometiendo un fraude”. El proveedor de servicios de Internet nos daba esa identidad sin utilizar ningún proceso. Y entonces la gente que estaba en el chat se tenía que enfrentar a los tribunales. Y decía, “Bueno, no me están dando ningún derecho para poder defenderme”. Y, en realidad, eran enviados ante los tribunales porque eran Juan o Pedro que habían cometido algo. Entonces la transparencia es algo a tener en cuenta, pero en ese caso se revelaba la identidad y se ponía en peligro la seguridad y la integridad de la persona.

Entonces por eso no se permite a los proveedores de Internet brindar información o revelar la identidad sin dar a los usuarios la posibilidad de defenderse.

Entonces, quizá mi idea no fue lo suficientemente concreta pero sí tenemos que seguir explorando un poco más estos mecanismos.

ABDULARIM OLOYEDE: Yo vengo de una parte del mundo donde sufrimos abusos, usos indebidos, etc. Y comprendo el hecho de que Internet es la voz del ser humano común. Pero creo que los activistas de derechos humanos y aquellos que se consideran parte de la sociedad civil son personas que a menudo se ponen en riesgo, porque con cada acción que uno hace hay un riesgo. Entonces, creo que los activistas de derechos humanos, y los activistas en general, son personas que salen y se expresan. Muchas veces hay otros que lo hacen dentro del anonimato de Internet.

Entonces mi pregunta es la siguiente. ¿Usted piensa que se debería hacer una defensa de esta característica anónima?

JONATHAN ZUCK: A ver, no vamos a responder a esta pregunta porque es muy amplia, es una pregunta sumamente amplia realmente. Yo quiero enfocarme en el tema del cumplimiento de la ley, que va a ser más sencillo de abordar. Ahora bien, agradezco a todos la participación. Vamos a continuar debatiendo.

La siguiente categoría o la siguiente diapositiva dice esto. Nos olvidamos cuáles son las diapositivas, parece.

Bueno, la siguiente categoría tiene que ver con la ciberseguridad, los recursos, la investigación y sistemas de reputación. Yo lo dividí en diferentes categorías, pero probablemente estén dentro de lo mismo. Entonces, en lugar de esperar a que aparezca la diapositiva, vamos a compartir parte de los datos, así que le doy la palabra a Greg.

GREG AARON: Yo soy miembro del SSAC de la ICANN y también soy representante del SSAC ante el EPDP. En mi trabajo diario soy un profesional que se desempeña dentro del área de la ciberseguridad. Me dedico a detectar y a mitigar los usos indebidos dentro de Internet y en el espacio del DNS específicamente. También hago investigación en el Grupo de Trabajo Anti-Phishing.

Hay diferentes puntos de vista con respecto a cómo la gente se ve afectada en este nuevo mundo. Debemos decir que muchas de las cosas que se hacen para proteger a los usuarios en Internet las hacen la industria. Es decir, la investigación consiste en determinar cuáles son los problemas, los usos indebidos, los delitos cibernéticos y abordar estas cuestiones de diferentes

formas. Entonces, utilizar los datos de diferentes maneras ayuda a resolver problemas.

El cumplimiento de la ley también participa en muy pocos de los casos que tienen que ver con las cuestiones de ciberdelito o uso indebido. A veces encontramos algunas cuestiones. Pero muchos de los problemas en realidad son abordados por las personas que controlan los recursos de Internet. Internet es una red de redes, y esas redes son compañías, universidad, gobiernos. Otras entidades que brindan servicios dentro de Internet. Y básicamente son ellos los que abordan o lidian con la cuestión del ciberdelito. Y esto implica también determinar qué es lo que uno quiere. Hay ciertas cosas a las que uno no quiere que los usuarios accedan dentro de la red como, por ejemplo, sitios web que son falsos. Esto es parte de lo que hacen los investigadores de ciberseguridad.

Dar de baja algo es parte importante porque en realidad hay muchos nombres de dominio que son fomentados por delincuentes y que no pueden continuar existiendo.

Ahora, ¿tienen idea de cuántos nombres de dominio son registrados por criminales o delincuentes anualmente? Bueno, millones realmente. Hay números que se enumeran en estas líneas de bloqueo que tienen los proveedores de Internet. Todos estamos protegidos de alguna manera teniendo en cuenta estas

listas, estos nombres. Bueno, no lo ingresamos en los buscadores, sabemos que tienen que ver con *phishing* o con malware. Pero quizás el número sea mucho mayor porque los investigadores solamente pueden encontrar una cierta cantidad o porcentaje de los nombres de dominio que están registrados.

Una de las formas en las que nosotros nos damos cuenta de esto o uno de los principales indicares que tomamos en cuenta es el WHOIS. Cuando se registran no ponen nombres reales. Pero así se puede identificar a nombres de dominio que son sospechosos, mediante la validación o verificación de ciertos datos. Entonces esto también resulta un indicador para nosotros teniendo en cuenta, por ejemplo, la información de contacto que se coloca dentro del WHOIS.

Entonces, básicamente este es un indicador fundamental. Uno puede tratar de buscar nombres de dominio que no son correctos con otras formas, pero ha sido durante muchos años una herramienta muy útil el WHOIS. Y no solamente nos ayuda a determinar cuáles son los dominios a tener en cuenta, pero también muchas veces nos ayuda a determinar quién está detrás de determinada actividad.

Si me permiten, quiero mostrarles unas diapositivas. Este gráfico muestra lo que sucedía antes y después de la entrada en vigencia de la especificación temporaria. En este caso es una lista de

bloqueo de nombres de dominio, entonces lo que muestra el gráfico es que la cantidad de nombres de dominio que se podían identificar y que estaban enumerados oportunamente antes y después de la entrada en vigencia de la especificación temporal cambió. Antes está reflejado en gris y después está reflejado en rojo. Esto implica que uno perdió la capacidad de poder identificar o de encontrar estos nombres de dominio. Esto representa un 67% aproximadamente.

Esto significa que se pueden buscar menos nombres de dominio y que, por lo tanto, hay gente o más personas que son más afectadas por estos nombres de dominio que operan incorrectamente porque no se los puede identificar.

Aquí vemos en SUBRL dos nombres, US and GDN, donde los registros no expurgan los datos de contacto, es decir, se los puede ver. Aquí entonces SURBL pudo encontrar y listar los nombres de dominio que eran usados para hacer *spamming*, *phishing* y *malware*.

Aparece entonces cierto éxito cuando se encuentran los datos. Y en la última diapositiva, ¿qué vemos? El éxito completo. SURBL tuvo el mismo patrón que Spamhaus pero peor. Antes de la especificación temporaria es azul. Rojo después. Se perdió entonces la capacidad de encontrar muchos nombres de dominio. Y el número de nombres listados en la lista negra baja.

Y eso significa más daño para los usuarios. Ahora que tenemos una perspectiva desde mayo pasado, empezamos a ver los efectos.

Cuando tenemos estos problemas en la Internet, la velocidad es un factor esencial. Queremos encontrarlo lo antes posible porque queremos bloquearlo o cerrarlo. Si no lo encontramos rápido, significa que los criminales podrán, en gran medida, hacer lo que se les ocurra. Y es un problema.

Otra cosa que tenemos que tener en cuenta es que, en general, los criminales suelen registrar más de un nombre por vez. Ha habido casos según nuestra investigación donde una entidad criminal registró 100000 nombres de dominio por vez. Y si se los encuentre y se establece qué hacen, es muy bueno hacerlo porque les aumenta el costo y les reduce el número de recursos que usan para dañar a la gente. Y el WHOIS es la mejor manera de hacer este tipo de trabajo. Pero reaccionar a posteriori es un problema. Entonces, la velocidad y encontrar los sitios es lo más importante.

¿Cómo hacemos para tener las herramientas que necesitamos y a la vez cumplir con la ley? Esa es la gran pregunta que exploramos en la fase dos del EPDP.

El GDPR por omisión dice que los datos deben ser protegidos, que el sujeto de datos tiene el derecho de que esos datos sean protegidos y controlados, pero el GDPR explícitamente dice que hay usos legítimos de los datos los cuales deben ser balanceados con el derecho a la privacidad.

El GDPR enumera algunas de estas características que dan este equilibrio. Y dice específicamente que usos tales como protección de la red, identificación y prevención de fraude y reportar problemas a los organismos de aplicación de la ley son usos generales. Entonces la ley dice que los datos pueden ser utilizados de esto manera. Ahora el reto y el interrogante es, ¿Cómo equilibrarlo? ¿Cómo hacerlo con equilibrio?

La idea del acceso acreditado es dar algún tipo de marco que las partes privadas pueden recurrir para buscar los datos. La idea general es que tiene que ser un marco legal por el cual las partes se vinculen con ciertas obligaciones, que son en general de cumplimiento con el GDPR.

Por ejemplo, en un marco de este tipo, habrá que explicar por qué se está solicitando un registro. Y esto tiene que quedar registrado. Tendrá que haber algún tipo de retención de los datos. El GDPR estipula que solo se podrán tener los datos mientras se estén utilizando y que, eventualmente, cuando se termine el uso habrá que borrarlos.

Todo esto tendrá que incorporarse al marco, pero la idea es tener este marco por el cual las partes estarán obligadas a cumplir con las reglas. Y también tiene que ser auditable. Esto también tiene que ser parte del marco. No es cuestión de decir simplemente la parte X ahora tiene permiso para ver los datos y listo. No. También tendremos que ver cómo hace la parte su trabajo y, si no lo hace bien, habrá que pagar algún tipo de penalización. Tendrá un costo, como por ejemplo perder el acceso.

El GDPR, en general, habla de marcos de acreditación. El problema es que nadie realmente se ha puesto a conformar, a crearlos y desarrollarlos, porque es algo muy nuevo y no hay mucha experiencia. Entonces, eso será parte de las discusiones que tendremos en la fase dos, que requerirá asesoramiento jurídico. Algunos detalles que estipulen cómo circularán los datos. Tendrá que haber un organismo de acreditación que revisé las solicitudes de los investigadores, que revise esas acreditaciones de manera continuada, etc.

Entonces, el GDPR parece ser que permite que se hagan estas cosas. El interrogante es dónde está el equilibrio correcto. Y en la práctica, cómo se cumplen con todos los requisitos legales.

Pero si conseguimos responder estas preguntas, quizá tengamos una solución que nos permita aprovechar lo mejor de los dos

mundos y cumplir a la vez con lo que el GDPR dice que debemos hacer. Gracias.

JONATHAN ZUCK: Gracias. Yesim, ¿podemos ir a la siguiente de mis diapositivas, rápidamente? Las vamos a publicar. Aquí hay dos vínculos. Es una columna de Mueller que habla de los datos que mencionaron los panelistas, algunas instancias de cierres y otro vínculo de *block listing*, un vínculo con un blog que contiene estos dos estudios y los gráficos asociados; cpwg.wiki/mueller y cpwg.wiki/blocklisting son dos fuentes de información de los temas que hemos discutido. Mueller, que les pertenece a ustedes, me acabo de enterar. Acaba de hacer este blog. No sé si ustedes quieren hablar de esto. Fue mucha la información y es muy nuevo.

FARZANEH BADII: A ver, este mundo puede ser fáctico, puede haber una compañía que tenga un registro en 2018 después de tres meses del GDPR y haya reportado que el *spam* cayó.

Puede haber otra compañía que ha expurgado un registro pero que el *spam* no ha afectado en números significativos.

Hay otros datos que han sido emitidos por otras compañías que dicen que el *phishing* ha disminuido. Pero, como decía, me parece que no deberíamos poner el énfasis en encuestas y en los datos, porque aparecerá después otra fuente de cifras y no podremos llegar a una conclusión.

Tendremos que ver esto dentro de un año o dos y ver realmente cuál es el efecto. Que lo haga una organización neutral que no tenga intereses involucrados.

No creo que estas estadísticas puedan ayudarnos a resolver la cuestión. No quiero desvalorizar el trabajo que hacen los investigadores en ciberseguridad porque muy bueno, pero no alcanza con decir que un problema ha disminuido porque se ha expurgado o no un dato.

Por otra parte, Paul Vixie, que es un investigador de ciberseguridad, dijo que el WHOIS quizá no se hubiera necesitado para manejar los ataques de ciberseguridad o no se necesite en el futuro.

Esta es mi opinión personal. Por supuesto, ese señor quizá no opine lo mismo. Cuando vemos estos datos, estas estadísticas, tenemos que tener una mirada objetiva. Y quizá tomarlo con pinzas. No digo decir que el trabajo no es importante y que

nuestro trabajo sí lo es, sino identificar cuál es la parte integral de la ciberseguridad.

GREG AARON: Creo que en el desarrollo de políticas en la ICANN es necesario contar con datos y hechos. Y, en mi opinión, no lo hacemos con la extensión suficiente. Lo que estamos haciendo ahora es empezar a recopilar los datos. Ahora por ejemplo podemos comparar el antes y el después. No creo que sea una buena idea necesariamente matar al mensajero en este caso, porque el mensajero es el que tiene el dato.

Por un lado, vemos que la detección ha caído en algunos de estos lugares. Pero si vemos la cantidad de mensajes de *spam* que se están enviando en la Internet, parece ser bastante constante. Así que sigue habiendo actividad, pero no tanto como antes.

Entonces los datos son importantes. No son siempre impunes los motivos de la gente para recopilar y analizar los datos. Gracias.

KATHY KLEIMAN: Le pregunté antes a Jonathan si había algo que debíamos revisar. Yo lo que sugiero es que revisemos estas diapositivas juntos, no ahora. Pero quizás encontrar algún espacio.

Elliot Noss, el Presidente de Tucows, dos meses después del GDPR, nos dijo que un tipo de delito había bajado, que era el envío de millones de mensajes *spam* a registratarios diciendo que los nombres de dominio habían expirado. Pedía poner el nombre, la dirección… había millones de mensajes de *spam*. Y hoy en día casi no existen. Eso bajó mucho.

Paul Vixie, que es uno de los creadores del DNS, un pionero de la investigación de la seguridad del DNS, declaró que esto era obsoleto, que el WHOIS no era necesario para la investigación de gran envergadura del DNS.

Tengo una pregunta para Laureen, Greg y para todos ustedes. Les pregunto, ¿qué es un investigador en ciberseguridad? Y ese es un problema, porque no hay credenciales. Tenemos que preguntarnos entonces, ¿cualquiera que se autodenomine investigador en ciberseguridad lo es? Este es un problema que hemos tenido en el pasado. ¿Tenemos que chequear la membresía en grupos de membresía como el Grupo de Trabajo Anti-Phishing? ¿Qué y cómo harán estos grupos para que sus rindan cuentas y sean responsables en el futuro?

GREG AARON: Gracias por la pregunta, Kathy. Nosotros también lidiamos con esta pregunta. El SSAC 101 trata algunos de estos temas. Es como

un profesional de la seguridad, la definición. En nuestro punto de vista, es una persona que tiene una responsabilidad profesional de ocuparse de estos problemas. Pero la pregunta es que incluso esta definición puede no ser suficientemente restrictiva.

El acceso a los datos asume ciertas responsabilidades que deben definirse. Algunas personas o entidades entonces quizá no cumplan con el nivel de responsabilidad y auditoría de manejo de los datos que son necesarios para ello.

¿El APWG pensó entonces quizás en algún organismo de acreditación para examinar a los miembros? Sabe quiénes son los miembros y qué relaciones existen, pero no todos tienen las capacidades para hacer las cosas bien y manejar los datos. Entonces tendremos que elaborar un proceso de aplicación y de evaluación largo para determinar quién puede hacer esta tarea y luego revisar el trabajo de manera regular. Y, nuevamente, construir algún tipo de capacidad de auditoría y ese tipo de cosas. Es un grupo amplio. Pero la gente que puede hacer estas cosas bien, será un grupo pequeño.

COLLIN KURRE: Hola. Soy Collin Kurre y quería hacer una intervención muy breve. Entiendo lo que usted dice, la necesidad de tener datos. Y quería marcar algo que dijo la comunidad del modelo de desarrollo de

modelos de impacto que podrían usarse. Este equilibrio entre anonimidad, entre seguridad y privacidad. Y quería resaltar el trabajo que hacemos para tener un diálogo más constructivo. Gracias.

JONATHAN ZUCK: Es importante porque tenemos que discutir esto, porque tenemos que dar asesoramiento a la Junta y porque existe además la urgencia de la fase dos. Por eso estas cosas entran en juego. Olivier creo que es el siguiente. Olivier, Hadia, Holly, Humberto y Andrei. Y con esto cerramos la lista.

OLIVIER CRÉPIN-LEBLOND: Muchas gracias, Jonathan. Mi pregunta es una pregunta que tenía en mente, que es, ¿cuántos datos de registración se usan para poder calificar a un nombre de dominio como fuente de *spam* y malware? Imagino que hay otras formas, como *honeypots* u otras herramientas. Quizá sea el momento de repensar las maneras en las que detectamos el *spam,* el malware. Quizá la inteligencia artificial. No voy a decir que vamos a usar *block chain*. Pero, inteligencia artificial, ¿por qué no?

GREG AARON: Gracias por su pregunta. WHOIS es una de las herramientas que se usa, pero no es la única. Hay todo un conjunto de mecanismos de calificación o puntaje que se utiliza. Por ejemplo, qué direcciones de IP. Una manera de encontrar *spam* es a través de los señuelos, de los *honeypots*. Las cosas que se publicitan. Esos son los nombres de dominio que más nos preocupan. Hacia los nombres de dominio donde se envían, ahí se harán los delitos.

A veces, esos son indicadores de problemas. Y también queremos saber qué otros nombres de dominio usan para el mismo esquema, porque la meta es evitar el daño lo antes posible.

La gente que hace esto hace mucha heurística, hace mucha correlación. Hace inteligencia artificial y no usan *block chain*.

OLIVIER CRÉPIN-LEBLOND: Prometo que no voy a hacer más preguntas después de esta. Los registros del DNS tienen los datos de servidores de nombres y también los registros de SOA. ¿Es suficiente esto para establecer un paralelo?

GREG AARON: No, no. Y una de las razones es porque un criminal configura su nombre de dominio en un servidor por omisión, como el que le da el proveedor de servicios. Y luego cambia el servidor de nombres cuando empieza su trabajo criminal. Hay una conmutación. Y eso

lo sabemos porque la gente va a los archivos de zona y hace *queries*.

Ellos también saben lo que nosotros hacemos. Es como el juego del gato y el ratón permanente. Y lo que nos preocupa hoy día, como perdimos una herramienta importante, es que la gente va a comenzar a sobrebloquear o compensar de otras maneras, y esa quizá no sea una buena idea. Hay operadores de red que en este momento están empezando a bloquear TLDs completos. Todos los nombres de dominio de TLDs que vienen de este TLD los bloqueamos. Y esa no es una buena idea. Queremos la aceptación universal, pero vemos que la gente empieza a usar soluciones que quizá no sean tan precisas y que pueden tener efectos no pretendidos, distintos de los esperados.

JONATHAN ZUCK: Gracias. Nosotros tenemos nuestros propios debates internos que debemos dejar para otro momento. Pasemos a Hadia.

HADIA ELMINIAWI: Tenía una pregunta para Greg. ¿Cuántos necesitan los datos históricos para sus investigaciones? ¿O, de hecho, necesitan datos históricos para empezar? También quería reiterar lo que dijo Greg respecto del GDPR y los intereses legítimos.

Artículo 48 del GDPR dice que la prevención del fraude constituye un legítimo interés. Y el 50 también habla de la seguridad de la red y de la información. Gracias.

GREG AARON: Los datos históricos son útiles en investigaciones que se hacen en profundidad, en especial cuando tratamos de determinar quién es el responsable. Los organismos de aplicación de la ley también lo hacen. Y en algunos queremos casos queremos saber quién es el autor del delito. Eso es importante. La mayoría de las cosas que se dan en tiempo más real, bueno, ahí los datos actuales son los que utilizamos.

JONATHAN ZUCK: Tiene la palabra Holly.

HOLLY RAICHE: Tengo algunas preguntas. En primer lugar, la forma en la cual describe lo que se hace puede ser posiblemente delictiva, pero también puede no serlo, y creo que el GDPR y las agencias de cumplimiento de la ley determinan dónde se clasifica cada cosa. ¿Esto es así? Esa sería mi primera pregunta.

Y en cuanto a las fuentes de excepción con respecto a quién tiene acceso a los datos y qué tipo de definición es lo suficientemente

amplia para que haya suficiente protección con respecto a los datos que se tienen para poder también abordar lo que decía Kathy, ¿qué definición sería la adecuada para las excepciones? Porque tenemos a las agencias de cumplimiento de la ley, por un lado, pero para mí las agencias de cumplimiento de la ley también son aquellas agencias que son responsables de quizás infringir la ley al poner riesgos a cierta parte de los consumidores, teniendo en cuenta la forma en la que se interpreta el GDPR.

También tenemos que tener en cuenta cómo se identifican las excepciones. ¿Pudieron abordar este tema? Creo que Kathy tiene la respuesta porque está sonriendo.

JONATHAN ZUCK: A ver, voy a desglosar un poco la pregunta. Creo que lo que usted pregunta es lo siguiente, que teniendo en cuenta las excepciones que hemos mencionado, usted cree que el GDPR da espacio a que los actores que no tienen que ver con el cumplimiento de la ley participen activamente. ¿Correcto?

GREG AARON: Bueno, como mencioné, muchas de estas funciones no son funciones del cumplimiento de la ley. La protección de las redes no es una función de las agencias de cumplimiento de la ley, es una función de la gente que está trabajando y operando con las

redes. El cumplimiento de la ley puede perseguir o tratar de entender quiénes son unos determinados clientes, los métodos de pago…

JONATHAN ZUCK: Bueno, pero, ¿usted piensa que el GDPR entiende esa distinción? Porque si no, ahí tendríamos que entrar en otro debate dentro de At-Large.

GREG AARON: Creo que está claro. Fue redactado específicamente para poder permitir acceso. Pero bueno, recordemos que más allá del GDPR hay otras leyes que tienen que ver con el cumplimiento de la ley y que también abordan cuestiones o leyes de privacidad. El rol de la industria creo que es fundamental.

LAUREEN KAPIN: Pero las agencias de cumplimiento de la ley no son las únicas que tienen la posibilidad de solicitar acceso según el GDPR.

HOLLY RAICHE: Yo le voy a pedir a Jonathan que interprete lo que yo quise decir porque veo que no entendieron mi pregunta.

JONATHAN ZUCK: A ver, creo que lo entendieron, pero no del todo. El GDPR toma en cuenta otros agentes que no son agencias de cumplimiento de la ley. Esta es la respuesta a la pregunta. Pero bueno, vamos a seguir avanzando. Quiero dar la palabra a Humberto antes de que perdamos la traducción.

HUMBERTO CARRASCO: Voy a hacer una pregunta muy breve. Es una pregunta y un comentario. Parece que hay un contraste entre el lado izquierdo y el lado derecho, desde mi punto de vista de los planteamientos, particularmente en cuanto a los datos, y creo que hay un error en el punto de vista porque Kathy habló y citó algunos datos en el descenso en el *phishing* y también el descenso en la cantidad de *spam* desde que entró en vigencia GDPR.

Pero, por otro lado, hay un reclamo de Greg en el sentido de que hay una imposibilidad de acceder a los datos, pero me da la impresión de que este es un aspecto preventivo de la situación. O sea, ha disminuido porque no se ha podido acceder a los datos. En el caso contrario se dice mire, una vez que se ha cometido el supuesto delito, vamos a nombrarlo así, nosotros no podemos acceder a investigar. Pero eso es reactivo. Entonces por eso yo pienso que hay un problema en cuanto a que están discutiendo dos temas absolutamente distintos en una sola línea, y a mi juicio eso parece un error.

JONATHAN ZUCK: Sí, correcto. Vamos a discutirlo luego. Le voy a dar la palabra al siguiente orador, Andrei.

ANDREI KOLESNIKOV: Mi hija trabaja para una empresa privada que se encarga de cuestiones que tienen que ver con el *spam* y ese tipo de cosas, y también trabaja con los registradores a diario. Para darles una idea, la empresa tiene 25 años. Y hace mucho tiempo que trabaja con la industria de Internet. Tiene trabajadores muy jóvenes también. Muchas veces tienen que tratar con agencias de seguros, aerolíneas, empresas grandes y pequeñas. Tienen que tratar también el tema del WHOIS. Y gracias a que el WHOIS todavía sigue operando, muchas de las solicitudes se pueden resolver. Muchas veces tenemos resultados por parte de los registradores rusos, pero la mayor parte de la información viene de otros registradores importantes como GoDaddy. Entonces esto nos ayuda a identificar los nombres que son incorrectos. Por ahora funciona todo bien, pero ya se ha comenzado a ver el impacto de los cambios porque la reacción se hace más lenta. Los tiempos de reacción son diferentes.

No vamos a decir que todo se cayó, pero sí se percibe una diferencia que ya se puede ver. Simplemente quería mencionar eso.

KATHY KLEIMAN: Es una observación muy válida, por supuesto. El tiempo de reacción es menor porque los registradores, según el GDPR, tienen que evaluar la necesidad y el derecho del solicitante y del registrador. Entonces hay una intervención humana. Olivier, no tenemos inteligencia artificial implementada en esto, pero vamos a trabajar en el tema.

Entonces, por definición, no es algo automático, no es una base de datos que se consulta. Por lo tanto, esto hace que los plazos sean diferentes y sean más lentos. Pero la idea es crear un sistema un poco más automatizado. Esto es algo sobre lo que hemos estado debatiendo.

FARZANEH BADII: El solicitante tiene que ser considerado responsable y –

ANDREI KOLESNIKOV: Esto se hace con cartas oficiales, firmadas, ¿cómo se hace?

FARZANEH BADII: Sí, por supuesto, todo depende, las urgencias se tratan primero y son más expeditivas.

JONATHAN ZUCK: Desafortunadamente, ya nos quedamos sin tiempo. Hay gente que está tratando este tema desde hace muchísimos años. Gente que ha pasado más de la mitad de su vida abordando este tema. Nosotros nos hemos quedado sin tiempo. Les quiero agradecer a los panelistas su participación. Gracias por respondernos. Tenemos mucho debate por delante. Probablemente en breve nos reunamos para hablar de este tema del EPDP. Ahora tenemos más información. Por supuesto, les agradezco la información a todos los colegas que nos la han dado.

FARZANEH BADII: Gracias, Jonathan. Agradezco la invitación. Es muy importante para mejorar nuestra relación con At-Large. Es importante que ustedes incluyan nuestra perspectiva aquí. Para nosotros es sumamente importante. Gracias.

JONATHAN ZUCK: Gracias al personal técnico, a los traductores, por quedarse más tiempo. Gracias a todos. Ahora pueden ir a comer.

JOHN LAPRISE: La próxima sesión empieza a las 12:15. Son las 12:10, así que no vamos a tener un receso de 15 minutos porque va a comenzar la próxima sesión, que es el almuerzo de At-Large, a las 12:15.

[FIN DE LA TRANSCRIPCIÓN]