BARCELONA – Sesión intercomunitaria: GDPR
Miércoles, 24 de octubre de 2018 – 09:45 a 12:00 CEST
ICANN63 | Barcelona, España

ORADOR NO IDENTIFICADO: Le pido a los miembros del panel que tomen asiento, por favor. Estamos listos para comenzar. Greg Milton. Chris.

BRUCE TONKIN: Vamos a comenzar para poder usar el tiempo de la mejor manera posible esta mañana.

Yo soy Bruce Tonkin, y me pidieron que presidiera esta sesión intercomunitaria sobre GDPR. El concepto de una sesión intercomunitaria es reunir a la comunidad para tratar de ver cómo la comunidad en su totalidad puede centrarse en problemas importantes y resolverlos. En esta sesión intercomunitaria tenemos representantes de varias partes de la organización de la ICANN. Tenemos representantes de la GNSO, responsable de políticas relacionadas con los nombres de dominio Gtld.

Del lado de la cámara de partes contratadas, tenemos a Nick Wenban-Smith. Nick es el miembro del consejo designado en Nominet y también es el abogado general de Nominet. Él trabaja en nombres de dominio genéricos, como .BLOG y también nombres de dominio de código de país como .UK.

Luego, del lado del Grupo de Partes Interesadas Comerciales, tenemos a Flip Petillion. Flip es de una empresa belga que ofrece servicios de resolución de disputas y también está involucrado en la resolución de disputas relacionadas con los nombres de dominio.

Del lado del Grupo de Partes Interesadas No Comerciales, tenemos al profesor Milton Mueller, de Georgia Tech en Atlanta, Georgia.

Del lado del Comité Asesor de Seguridad y Estabilidad tenemos a Greg Aaron. Greg es vicepresidente de iThreat Cyber Group y trabaja en el grupo de ciberamenazas y también trabaja en la agencia de amenazas e investiga el uso de nombres de dominio para el uso indebido *online*.

Del lado del Comité Asesor At-Large, tenemos a Hadia Elminiawi. Del lado del Comité Asesor Gubernamental tenemos a Ashley Heineman. Ashley es responsable de políticas de Internet dentro de la NTIA en Estados Unidos. Y el GAC tiene un desafío difícil al analizar cuestiones como la privacidad y cómo lo manejan los diferentes miembros del gobierno que son miembros del Comité Asesor Gubernamental y cómo encuentran soluciones que son relevantes a nivel global.

También tenemos a un representante del Grupo de Partes Interesadas de Aplicación de la Ley, Chris Lewis-Evans. Chris trabaja en la Agencia Nacional de Delitos del Reino Unido y es responsable de las investigaciones en Internet.

Del lado de la protección de datos, tenemos a Cristina Monti. Cristina forma parte de la unidad de Flujo de Datos Internacional y la Dirección de la Comisión Europea para la Protección de Datos.

Todos los miembros del panel han estado involucrados durante muchos años en el manejo de los desafíos que tienen que ver con la protección de la información personal.

Me pareció que, en primer lugar, sería útil establecer el contexto. Y probablemente sea pertinente volver al RFC-1591, redactado por Jon Postel en 1994. Y, de hecho, ahora celebramos el vigésimo aniversario del fallecimiento de Jon Postel, que murió el 16 de octubre de 1998. Es interesante ver lo que se escribió hace más de 20 años.

Y en el RFC, Jon estableció que los administradores de dominios de alto nivel son los fideicomisarios de nombres delegados.

Él también dijo que las preocupaciones con respecto al derecho y a la titularidad de los nombres de dominio es inadecuado. Lo adecuado es preocuparse por las responsabilidades y servicios prestados a la comunidad.

Por lo tanto, tenemos a los titulares de los nombres de dominio de alto nivel y los titulares registrados son responsables de cumplir con la ley en sus jurisdicciones locales. Algunos son personas naturales, en el contexto de los titulares registrados también hay personas naturales.

Y también los datos de estas personas naturales se ven protegidos bajo diferentes leyes de privacidad en distintos países del mundo.

¿Dónde encaja la ICANN dentro de este tema? La ICANN tiene una misión muy definida, que es coordinar la asignación de nombres en la zona raíz. Estoy eligiendo las partes de la misión que son pertinentes para este tema. Pero la asignación de nombres en el DNS opera la

asignación de nombres de alto nivel. Y también coordina el desarrollo y la implementación de políticas relacionadas con la registración de nombres de dominio en los gTLDs.

Queda muy claro en las [Inaudible] de la ICANN que la ICANN no va a regular los servicios que utilizan los identificadores únicos de Internet ni tampoco el contenido.

Por lo tanto, son otros en general los organismos de seguridad y otros organismos de aplicación de la ley los que deben tomar medidas en caso de que se viole la ley.

En este sentido, estas autoridades dependen de organizaciones del sector privado como las organizaciones de ciberseguridad que recaban información acerca de incidentes que permiten realizar investigaciones adecuadas.

Es interesante también hablar acerca de WHOIS, que es lo que reúne a todos para hablar acerca de cómo vamos a considerar la próxima generación de información que vamos a brindar en un registro. Yo leí el RFC original de WHOIS, que no es el 92.

Y de hecho era un servicio de directorio para las personas que utilizaban ARPANET en ese momento. Y exigía el nombre, la dirección, el número de teléfono y el correo electrónico. Entonces, lo interesante es que ni siquiera se llamaba *e-mail* en ese momento. Se llamaba *mailbox* de red.

Y fue evolucionando, se convirtió en una fuente de contactos para las personas administrativas y técnicas para los nombres de dominio

para una serie de instituciones muy conocidas. Ahora la situación cambió. Tenemos cientos de millones de registraciones de dominios y, en lugar de tener grandes instituciones, muchas veces son registradas por personas y muchos que actúan en su propio nombre. Pero aún tenemos que identificar la identidad legal, responsable por el uso del nombre. Y tenemos que tener un contacto del titular de quien registra el nombre para resolver problemas.

Y lo que muchas veces se olvida es que con frecuencia el titular del nombre de registro es la víctima y no el perpetrador de actividades en relación al nombre de dominio. En general, se *hackean* los sitios web, los correos electrónicos. Y cuando uno investiga un problema, con frecuencia resulta que el titular del nombre de registro no tiene nada que ver y, de hecho, necesita ayuda para resolver el problema. Por lo tanto, no es necesariamente el caso de que el titular del nombre haya ocasionado el problema en relación con el uso del nombre.

Creo que vale la pena reflexionar acerca de registros públicos similares, seguramente tienen características similares con los registros de los nombres de dominio de Internet.

Por un lado, tenemos los registros con información de empresa. Muchos países tienen legislaciones que requieren que aquellos que realizan negocios, que esas empresas se registren como empresas, como compañías; y la información recabada como parte de ese proceso con frecuencia son datos personales como la dirección, los nombres, los números de teléfono de personas individuales, etc.

Otro ejemplo son los registros de registración de automóviles. Acá es donde el registro incluye información acerca del vehículo, por ejemplo, el color, la marca, el modelo… y también datos personales sobre el dueño del vehículo, que podría ser una empresa o podría ser una persona física.

Y tenemos una analogía similar con la ICANN. Si pensamos en un organismo de registración de vehículos que maneja los identificadores únicos, que básicamente sería la patente de un vehículo, en este caso podrían ser identificables personalmente. Pero si alguien quiere ser contactado, va a pintar el nombre de la empresa en el vehículo. Pero, en general, la gente no pone su nombre personal en su vehículo.

Y si vemos quién es responsable de lo que se hace con el vehículo, en general, la licencia para usar el vehículo implica que uno puede manejarlo como quiere, puede poner lo que quiera dentro del vehículo, puede transportar cualquier cosa dentro del vehículo, puede poner cualquier persona dentro del vehículo. Pero las agencias que son responsables de emitir la patente no les importa eso. Lo que les importa es que puedan identificar a la persona que es dueña de ese vehículo.

Y hay otros organismos regulatorios, si el coche está estacionado en un estacionamiento y alguien de pronto observa que está lleno de droga, entonces la policía va a investigar y va a ir a la autoridad de registración para obtener información acerca de ese vehículo.

Si uno está involucrado en un accidente de tránsito, si alguien nos choca y luego se va, lo único que sabemos con respecto a esa persona

es la patente del auto. A partir de la patente, como miembro del público en algunos países, sé que en Australia y Reino Unido sin duda esto es así, uno puede ingresar el número de la patente y obtener información del registro acerca del vehículo. Y vamos a saber qué marca es el vehículo, qué modelo, qué color… pero no vamos a saber quién es el dueño del vehículo.

Pero esto nos permite asegurarnos de tener el coche correcto, porque quizá no recordemos del todo el nombre de la patente, quizá solo recordemos los últimos números y así podemos verificar si es el coche adecuado.

Una vez que sabemos que es el coche adecuado, ahí si podemos solicitar información a las autoridades de aplicación de la ley y decir que esa persona me chocó y se alejó, y luego las autoridades de aplicación de la ley pueden obtener información acerca de la persona física que potencialmente es dueña de ese vehículo.

Entonces hay muchas analogías con nuestra situación. A la ICANN no le importa lo que haya dentro de los sitios web. A la ICANN no le importa lo que haya dentro de los correos electrónicos que ustedes envían. De eso se ocupan otros. Lo único que le importa a la ICANN es que podamos recabar información sobre las partes que son titulares de ese nombre de dominio, que podamos contactar a esas partes. Y depende de otros llevar a cabo medidas de seguridad o de aplicación de la ley en relación con esos nombres de dominio.

Los registros de números telefónicos son similares en muchos países. Uno puede elegir no figurar en la guía telefónica. Los registros de

nombres de código de país son similares a la situación de los gTLDs. La diferencia es que operan dentro de una única jurisdicción. Y la mayoría de los registros de códigos de país en Europa, obviamente actualizaron la implementación de sus servicios de directorio para cumplir con el GDPR. Por lo tanto, podemos aprender de estos casos, pero, de todas formas, tenemos que buscar una solución que sirva a nivel global y no a nivel de cada país individual.

Para darles el ejemplo de Nominet, para que tengan una idea de cómo ellos manejan esto y cómo muestran información mínima en el WHOIS público. Ellos tienen acceso autenticado para los organismos de aplicación de la ley dentro del Reino Unido, pero no organismos de aplicación de la ley fuera del Reino Unido, para que puedan acceder a los registros de manera automatizada.

También hay un formulario en el sitio web que un usuario legítimo puede completar para tener acceso a la información, quizá tenga que explicar para qué necesita acceder a la información. Y luego Nominet evalúa cada caso de manera individual sobre la base de quién está pidiendo la información y cuál es el propósito, y hace una evaluación para ver si hay una legislación que lo apoye y luego brinda la información a la parte que la solicita.

Esto crea una solución que hace que se pueda cumplir con la ley en el Reino Unido y en Europa en términos más generales.

Los Registros Regionales de Internet también, en general, tienen información sobre la organización, que probablemente sea una empresa de telecomunicaciones, un proveedor de servicios de

Internet o, en algunos casos, grandes organizaciones que tienen rangos de direcciones IP. En general, los datos tienen que ver con el contexto de estas organizaciones.

Pero, por ejemplo, RIPE que está en Europa tiene que tener una solución que cumpla con GDPR.

Entonces, en términos del IETF, hay mucho código que se está escribiendo en este momento. Hay sistemas que están operando hoy y que cumplen con la legislación de los países en los que operan y con la necesidad de los requerimientos de privacidad.

Si vemos cómo evolucionó la legislación de privacidad, hay muchos países que tienen legislación para proteger los datos personales. Y básicamente se actualizó cuando comenzó a haber información escalable y fácilmente accesible. Antes, si uno quería acceder a información sobre una empresa, tenía que ir físicamente a la empresa y probablemente tardaba varias horas en obtener un solo registro. Hoy en día, uno puede acceder a ese registro desde acá. Yo estoy acá, en Barcelona, y puedo acceder al registro de una empresa británica. Por lo tanto, hoy es más fácil acceder y la cantidad de información es mucho mayor.

Hace unos 100 años, uno tenía fecha de nacimiento y fecha de casamiento. Para eso, uno iba a la iglesia. No había centralización. Había que ir a la iglesia para obtener esta información, a la iglesia en donde la persona nació o en donde falleció, y ahí estaba el registro. Hoy, los registros están más centralizados y hay millones de ellos.

Entonces, la tendencia global ha sido ir actualizando la legislación de privacidad. En Europa, en la década de los 50, después de la Segunda Guerra Mundial, existía la preocupación y había mucho uso indebido de información de identificación personal. Esto ocurrió durante la guerra. Entonces esto empezó a considerarse parte de los derechos humanos básicos.

En la década de los 80, hubo una convención para proteger el procesamiento automatizado de datos, es decir, el procesamiento a gran escala por medio de computadoras.

En la década de los 90, hubo una directiva de protección de datos, pero se implementó de diferentes formas en los diferentes países. Y el desafío para las empresas era que tenían que ver cómo se aplicaban las leyes en los diferentes países europeos y, por lo tanto, esto implicaba un gran costo de negocios.

El Reglamento General de Protección de Datos de 2016 apunta a tener un abordaje uniforme para todos los países, para que las empresas puedan implementar el sistema una sola vez y luego aplicarlo a todos los países europeos.

Entonces, básicamente es una estandarización de la legislación de privacidad. No es algo nuevo. A veces la gente dice que de pronto tenemos una nueva ley de GDPR que salió en 2016. De hecho, tenemos en Europa leyes de privacidad desde los 80, pero GDPR es una estandarización de todas estas legislaciones.

Entonces, los desafíos para la ICANN consisten en que necesitamos una definición clara de para qué se recaban datos. Creo que es importante diferenciar el propósito de recabar datos para un registro público, que es lo que pasaba en la época de Jon Postel en el RFC-1591. Los registradores ofrecen muchos servicios; publicación de datos en la web, diseño de webs, servicios de marketing. Recaban todo tipo de información para su uso comercial.

Pero lo que nos preocupa en la ICANN es que se recabe información que pueda convertirse en parte del registro público, es decir, parte del registro público.

Tenemos que decidir qué información se va a recabar. Por eso los filtros para el público general, información no autenticada, quién tiene acceso a la información, cuál es la información que tiene que estar disponible para usuarios legítimos con fines legales y cómo autenticar este acceso para los usuarios legítimos. Y nuestro desafío es generar una solución que funcione en todo el mundo.

Tenemos datos acerca de personas físicas que se ocultan en casi todos los países del mundo. Y tenemos usuarios que, con frecuencia, también están en países diferentes de donde están los datos.

Y tenemos leyes que se aplican a personas físicas y también leyes diferentes para empresas. Este es un desafío mucho más grande que desarrollar una solución para un solo país o para una sola región con un grupo de países.

Resulta útil refrescar los principios de privacidad del GDPR. Una vez más, estos principios son comunes a muchas legislaciones de privacidad. El concepto de transparencia, al usuario hay que explicarle por qué se recaban los datos, cómo se van a almacenar y procesar, cómo se van a divulgar y cómo se van a entregar a terceros.

El concepto de limitación de propósito. Solo hay que recabar datos con fines legítimos y específicos.

Minimización de datos que se limita solo a lo que es necesario. Y acá escuchamos diferentes comentarios acerca de que, por ejemplo, un registrador que recaba información para poder prestar un servicio de *email* no necesita necesariamente una dirección postal, porque el registrador nunca va a enviar nada por correo postal, sino que lo envía por correo electrónico. Entonces, si un registrador que no tiene ningún otro requerimiento de ICANN, le preguntamos qué necesita, nos dice que alcanza con la información de la tarjeta de crédito. Pero con fines públicos, quizá si sea necesario recabar más información. Y acá la comunidad tiene que decidir cuál es la información que hay que reunir.

Exactitud, los datos tienen que mantenerse actualizados. En la GNSO hay una norma que dice que todos los años el registrador debe recordarle al registratario y al titular del nombre y de los datos que están en el registro público, en el WHOIS, que debe actualizar los datos. El cliente tiene que poder actualizar esos datos. Este es un intento de mantener los datos actualizados y, obviamente, los registradores brindan servicios para que los clientes puedan venir en

cualquier momento y actualizar sus datos. Entonces, con respecto a la exactitud, básicamente estamos cumpliendo con GDPR para que la gente puede actualizar sus datos.

En cuanto a las limitaciones de almacenamiento, normalmente uno diría, en cuanto el cliente deja de pagar con la tarjeta de crédito, ya no es necesario seguir guardando esos datos porque deja de ser cliente. Pero el registro público, en general, tiene almacenamiento a más largo plazo porque hay cuestiones legales, como ataques. Y por esas razones, muchas empresas requieren que cierta información se conserve durante varios años para poder, por ejemplo, aplicar la legislación fiscal. Entonces, la limitación del almacenamiento apunta a definir cuánto tiempo necesitamos retener la información desde el punto de vista de la ICANN. Pero, durante la registración, y una vez que se venció la registración, ¿durante cuánto tiempo hay que conservar la información?

Integridad y confidencialidad, básicamente eso tiene que ver con la seguridad, los datos tienen que ser seguros.

Entonces, creo que una de las cosas que escuché con frecuencia en estos paneles es que la gente habla acerca de los requerimientos, y creo que esto es algo que ya se dijo varias veces. Tenemos que ver cuáles son los requerimientos más generales. Uno de los supuestos que vengo escuchando esta semana es que precisamos dar marcha atrás con el proceso de desarrollo de políticas. Está la tentación de extraer recursos de este proceso y centrarnos en este tema. Pero para que la ICANN funcione, tenemos que asegurarnos de que podamos los

recursos suficientes y de que podamos contribuir al proceso de desarrollo de políticas. Entonces, el supuesto es que vamos a tener éxito y que vamos a generar una política.

Cualquier solución que surja debe tener cumplir con las leyes de privacidad. El GDR es una de ellas.

Toda solución debe permitir que las autoridades de aplicación de la ley y las autoridades públicas puedan investigar y hacer responsables a los titulares de los nombres de dominio por esos dominios.

Toda solución debe brindar protección a las personas que están en riesgo. Muchas veces escucho historias donde se dice que un matrimonio se disolvió, había violencia, una de las partes se mudó a otra parte del mundo… y la idea es proteger este nuevo lugar donde va la persona para evitar la violencia. Así que hay que pensar en ese tipo de escenarios, y estos datos podrían causar daños si llegan a las personas incorrectas.

Se habla mucho de esto. Y creo que es claro que la comunidad técnica considera que RDAP es suficiente para lo que se necesita. Pero RDAP es solamente un lenguaje, es una forma de intercambiar información. No es una solución. Solamente un idioma que elegimos para intercambiar información. Pero tiene algunas características muy poderosas. Algunas de estas características son que apoyan el concepto de distribuir información en lugar de que esté centralizada. Y hay flujo de información estándar, que algunas veces dio problemas con el modelo de WHOIS antiguo, donde había algunos temas de implementación.

Es muy similar al EPP, un estándar desarrollado por registros y registradores para comunicarse. Pero no reemplaza a las políticas. Necesitamos las políticas para que RDAP pueda implementarlas.

Aquí hay otro supuesto, y es que los registros y los registradores son responsables por los datos que conservan. Ellos recolectan información por diferentes fines y no todos tienen que ver con los nombres de dominio. Y son responsables de cómo procesan esa información y cómo la comunican. Así que eso también es parte de su responsabilidad.

Supongo que la pregunta inicial para el panel, es habiendo tenido en cuenta todos estos antecedentes, otros registros públicos, ¿cómo se han tratado esos problemas de protección de los datos personales en diferentes registros? El tema de dar acceso a los usuarios legítimos a información que no está disponible para el público en general, qué protección existe, etc. entendiendo el contexto de las leyes de privacidad que se están implementando en todo el mundo. Creo que nuestro desafío es encontrar una solución en forma oportuna. Y la primera pregunta para el panel en realidad es, ¿qué barreras o impedimentos creen que impide, desde el punto de vista de la ICANN, encontrar una solución? ¿Qué podemos hacer desde la ICANN para superar esas barreras? Y, ¿qué pueden hacer ustedes, pues tenemos aquí cientos de personas reunidas, para contribuir y ayudar a los equipos de políticas y a las personas que están en los diferentes grupos de partes interesadas para llegar a una solución exitosa?

Doy la palabra a los miembros del panel para que expresen sus opiniones sobre posibles soluciones y sobre la forma de superar posibles obstáculos.

Ashley, adelante.

ASHLEY HEINEMAN: Voy a empezar a nivel general. No voy a hablar de información detallada. Creo que gran parte de los obstáculos, al menos los que yo enfrenté en el último año aproximadamente, tienen que ver con personas que vienen aquí con ideas preconcebidas acerca de lo que piensan y hacen los demás, cuáles son sus motivaciones. Y también lo que he visto es que, una vez nos sentamos con diferentes personas, especialmente personas que representan diferentes perspectivas e intereses de usuarios, cuando empezamos a discutir los temas, no estamos en posiciones tan distantes como creemos que estamos. Pero creo que debemos crear más oportunidades de comunicarnos en forma constructiva y trabajar en pos de un objetivo común y evitar estas situaciones en las que normalmente nos encontramos, donde nosotros expresamos nuestra posición. Y realmente no estamos tratando de encontrar un terreno en común. Yo soy optimista, creo que podemos superar estos obstáculos. En algunos lugares ya vi que se superaron. Pero este es un tema que existe desde hace mucho tiempo, que trae toda una mochila. Es muy difícil dejar todos estos preconceptos de lado y trabajar juntos de forma constructiva.

BRUCE TONKIN: Sí. El desafío es que las personas cuestionan nuestras motivaciones y usted está en esa posición porque tiene esa opinión, y la realidad es que la mayoría de las personas tiene opiniones que están bastante equilibradas cuando hablan en privado, pero a veces participan en los foros públicos y presentan una opinión muy extrema. Quizás una forma de encarar esto sea hacer una serie de preguntas. Entonces, en lugar de empezar a hablar con alguien de otro grupo de partes interesadas y decir, esta es mi posición y yo tengo la razón, quizá podríamos preguntarles acerca de lo que creen que es necesario, qué opinan… para encontrar un terreno en común. Creo que necesitamos mayores capacidades de facilitación y quizás habilidades en cuanto a hacer preguntas en lugar de expresar la propia posición. Eso podría ser útil.

MILTON MUELLER: Creo que el principal impedimento es muy claro para mí como miembro del EPDP, y es que algunas partes de la comunidad tienen la esperanza de que podamos recrear el antiguo WHOIS o de alguna manera lograr el acceso a los datos con la libertad y facilidad que existía en el pasado. Y, por supuesto, a lo largo de los 20 años que existió WHOIS, se fueron creando intereses e igualdad en cuanto al acceso a esos datos. Había empresas basadas en el acceso a esos datos. Entonces lo que pasa en el EPDP con mucha frecuencia es que terminábamos discutiendo el tema del acceso y todo se subordina a este interés por el acceso, cuando deberíamos estar hablando de otros temas.

Entonces, creo que el obstáculo se puede superar si simplemente nos concentramos, en primer lugar, en el primer paso que es completar la especificación temporaria o ponerle fin, por así decir, y decir qué datos deben ser recabados, con qué objetivos y qué elementos de datos son necesarios, cuándo deben ser transferidos. Y deberíamos poder llegar a un acuerdo sobre esto, si dejamos de lado la pregunta de acceso para el paso dos. La carta orgánica exige que hagamos eso de todas maneras.

Si no confundimos los objetivos de los registros y los registradores en cuanto a la recolección de datos con los intereses legítimos de terceros en cuanto al acceso de los datos y nos concentramos en la parte uno, respondemos las preguntas clave en la carta orgánica y después pasamos al tema del acceso, creo que vamos a avanzar más rápidamente. Pero si todos los debates de objetivos y todos los debates sobre la localización de datos se convierten en una batalla sobre el acceso que no podemos resolver por el momento, vamos a estar dando vueltas y vueltas durante mucho tiempo.

BRUCE TONKIN: Una pregunta al público. Ustedes dijeron que entienden que algunas personas piensan que hay que volver al mundo antiguo, al antiguo WHOIS. ¿Quiénes piensan aquí que esa es una solución posible? Que volvamos al WHOIS antiguo. Una persona. Entonces, creo que esto es un mito en realidad, así que estamos avanzando. Y usted tiene razón, Milton, si volvemos a los principios relacionados con las leyes de

privacidad, habría que habría con qué objetivo se recolecta la información y qué información hay que recabar.

FLIP PETILLION: Gracias, Bruce. Quisiera recordarles a todos lo que dijo Cherine Chalaby el lunes por la mañana. Él dijo que debemos buscar y lograr un equilibrio entre lo que necesitamos en forma colectiva y lo que queremos en forma individual. Creo que lo expresó de manera brillante. Y de eso se trata el GDPR. Creo que todos debemos recordar qué es el GDPR, de dónde proviene, cuál es su objetivo. Y, honestamente, cuando se debatía el borrador del GDPR, nunca se pensó en lo que estamos tratando hoy. Normalmente se pensaba en proteger a las personas de recibir publicidad no deseada, *spam*, etc. Pero no pensaron en los problemas que enfrentamos hoy.

Hoy todos los que participan en este debate deben pensar si realmente entienden cuál es el objetivo, y hay que tener en cuenta lo que yo quiero equilibrado con los intereses de otros. Yo no creo, como algunos parecen presentarlo, que sea una opción entre lo mejor y lo peor. Ahora hay un desequilibrio. Y este desequilibrio no es aceptable para algunas personas en la comunidad. Debemos volver a recuperar el equilibrio. Y una vez que comprendamos esto, podremos tener debates mucho más fructíferos. Se trata del equilibrio.

BRUCE TONKIN: Usted dice, entonces, que la comunidad debe aceptar que tenemos que buscar un equilibrio.

FLIP PETILLION: Sí. Todo el modelo de la ICANN está basado en consenso, en confianza. Queremos que haya confianza por parte de todos, y la confianza es la base del consenso. Y el consenso es la base del equilibrio. Equilibrio de intereses.

BRUCE TONKIN. Levantemos la mano, por favor. ¿Quién cree que debemos centrarnos aquí, en lograr un equilibrio entre poder proteger la información y poder brindar la información? Levanten la mano, por favor. Aparentemente hay una clara mayoría que opina así. Suena bien. Entonces creo que estamos diciendo que WHOIS, tal y como era en el pasado, bueno, no podemos retroceder, pero también estamos diciendo que para avanzar debemos lograr un equilibrio. Y creo que hay mucho apoyo entre los presentes a favor de esto. Entonces el supuesto con el que trabajamos es correcto, que tenemos que lograr un equilibrio.

¿Cómo creen que podemos lograr este equilibrio? Esa es la parte difícil.

FLIP PETILLION: Con mucha buena predisposición y no pensando solamente en lo que debe hacerse dentro de GDPR sino también lo que deben hacer otros grupos también, como la protección de los consumidores, autoridades de la ley, protección de niños. Hay otras leyes que también son aplicables, no solamente en Europa. No olviden que

tenemos una directiva de comercio electrónico en Europa que establece que hay que ofrecer de manera obligatoria información de contacto del titular del sitio web. En primer lugar, esto está totalmente en contra de lo que dice el GDPR, pero no es así, porque toda la legislación de Europa, ya sea una normativa, una directiva, una regulación, siempre establece que la implementación y la aplicación de la regulación, la normativa o directiva, debe lograr un equilibrio. Un equilibrio entre este y otros elementos del marco regulatorio aplicable. Entonces debemos considerar el panorama general, el escenario general.

BRUCE TONKIN: Debemos hablar de esto. Estos son ejemplos, los ejemplos que usted mencionó de cómo se logró el equilibrio, porque como yo dije en el ejemplo, los registros lograron un equilibrio entre la suficiente información al público para que pueda entender quién es responsable de un registro en especial y también dónde se puede buscar información más detallada, si es necesario. Hadia.

HADIA ELMINIAWI: Yo creo que los desafíos son los siguientes. Quiero hablar de los desafíos desde el punto de vista práctico porque ahora todos sabemos que los datos de registración ya no son abiertos. Son datos con acceso restringido que solo van a estar disponibles y solo van a ser divulgados teniendo en cuenta los intereses legítimos de terceros. Entonces, hablando del equilibrio, debemos tener en cuenta que el equilibrio es y será necesario, pero también debemos saber que

nosotros no somos los que vamos a ejercitar este equilibrio cuando hablemos de la divulgación de datos, cuando hablemos de la implementación. Además, dejando esto de lado –

ORADOR NO IDENTIFICADO: ¿WHOIS?

BRUCE TONKIN: ¿Usted está diciendo que no cree que nosotros tengamos que lograr ese equilibrio?

HADIA EL MINIAWI: Sabemos que es necesario el equilibrio y debemos equilibrar las necesidades de las personas que tienen intereses legítimos para acceder a los datos y los derechos de los registratarios. Pero cuando hablamos de la implementación y la divulgación, no somos los que vamos a buscar este equilibrio caso por caso, y no somos los que vamos a implementar esto ni crear este equilibrio en este momento.

En algunos casos, entonces, reconocemos el principio, reconocemos este hecho, pero desde el punto de vista práctico, cuando llegamos a la implementación y divulgación de los datos, nosotros no somos los que vamos a decidir en este caso si el equilibrio es exitoso o no. Debemos recordar esto. Es lo que yo opino.

Además, también quisiera hablar acerca de los desafíos desde otro punto de vista práctico. Todas las políticas que estamos desarrollando y todo nuestro trabajo debe tener un fin de práctico, debe ser

implementable y debe cumplir con el GDPR, pero debe ser implementable. Esto es muy importante. Si desarrollamos una política que nadie va a implementar y que no resulta práctica de implementar, esto no es útil. Y yo creo que para resolver esto debemos hacer algunas cosas. Por ejemplo, necesitamos procesos estandarizados de la industria. Esto es necesario para que funcione la red de registros, registradores y registratarios, los servicios de acreditación y cómo vamos encarar esto.

¿Y quién se va a ocupar de esto? Además, hay otros desafíos en relación con los riesgos de la responsabilidad de las partes contratadas. Si tenemos una política que no tome esto en cuenta, nadie la va a implementar.

Creo entonces que estos son importantes desafíos que deben ser considerados ahora y no más tarde. Entonces, mientras hacemos el trabajo de política que estamos haciendo, y espero que lleguemos a un consenso, a una solución que nos satisfaga a todos.

Pero después habrá que ver cómo se implementa esto, y creo que es mejor trabajar en eso ahora y no más tarde. Creo que ese es el principal desafío.

BRUCE TONKIN: Usted está diciendo que para llegar a una solución oportuna tenemos que tener en cuenta la política y hacer una política correcta o adecuada. Pero, para dar con una solución completa, también hay que pensar en la implementación. Entonces habría que pensar en la

implementación ya, no una vez terminado el trabajo de desarrollo de políticas, que habría que hacerlo en paralelo.

Nick.

NICK WENBAN-SMITH: Estoy aquí representando las partes contratadas. Creo que es muy interesante que alguien haya mencionado el riesgo para las partes contratadas.

Y realmente me gustó que la palabra "oportuna" estuvo entre comillas, porque estamos en octubre y la legislación entró en vigor en mayo. Así que una solución oportuna la tendríamos que haber tenido hace 12 meses.

Pero bueno, tuvimos muchos temas que tratar, y la especificación temporaria es algo con lo que las partes contratadas están satisfechas en términos generales. Cuanto antes se complete el proceso de EPDP para formalizar esto, mejor, porque allí tenemos acceso.

Pero ya estamos hablando de políticas de acceso, porque desde el 25 de mayo hemos tenido que cumplir con la ley y esto incluye el tema del acceso.

Entonces, uno de los desafíos interesantes del GDPR es que tiene que ver con los principios. Hay que tener un equilibrio entre los principios de interés legítimo con los principios de derechos de privacidad de los sujetos titulares de los datos. Y este es un desafío. Pero por necesidad, como no había ninguna política formal, tuvimos que tomar decisiones

nosotros mismos. Entonces, hay una especie de *patchwork* de diferentes políticas en cuanto a la divulgación de datos, y lo que hacemos en el Reino Unido es legal, porque recibimos cientos de pedidos de acceso. Y yo recibí también algunos reclamos. ¿Y cómo sabemos que estamos cumpliendo en términos de las leyes de protección de datos? A través del espejo retrovisor. A alguien no le gusta lo que hacemos, se queja a la autoridad de la protección de datos del país, que nos manda una notificación y nos dice, "Recibimos un reclamo".

Y yo recibí un reclamo sobre la divulgación de datos. Esto lo envió un organismo que se ocupa de la propiedad intelectual. Y el reclamo fue rechazado. Así que yo sé que mi proceso de divulgación es lo suficientemente sólido para, por lo menos, enfrentar los desafíos que enfrentamos. Es un ejercicio continuo ver el tema de si hay derecho a presentar reclamos o no.

En este momento estamos desarrollando un cuerpo de experiencia con respecto a lo que pasó después de la implementación de GDPR. Vamos buscando nuevas soluciones, porque sí, sabemos que recibimos solicitudes que no podemos satisfacer. En los últimos tres meses recibimos 750 solicitudes. El 96.5% aproximadamente las respondimos. Pero algunas personas piden la información sin explicar los motivos, así que no están cumpliendo con lo que establece el GDPR.

BRUCE TONKIN: A ver, estamos escuchando que hay decisiones que deben ser tomadas a nivel local, considerando que no pueden divulgar los datos de cualquier manera. Y también que ambas partes deben cumplir con lo establecido, digamos la parte que pide los datos debe pedir los datos de manera adecuada y puede reclamar si no los recibe, y la parte sobre la que se presentan los datos también puede presentar un reclamo.

NICK WENBAN-SMITH: Todo esto ya está establecido en la legislación.

BRUCE TONKIN: Muy bien. Greg.

GREG AARON: Gracias, Bruce.

Parte de las conversaciones que se están manteniendo esta semana tienen que ver con las responsabilidades que el GDPR impone a todos. Y esto es bueno.

Tiene que ver con la responsabilidad en cierta forma. Y también se convierte en un debate acerca de la gestión del riesgo. Todos tienen estas responsabilidades. Y, por supuesto, a veces hay penalizaciones asociadas cuando uno no cumple con sus responsabilidades.

El problema con la gestión del riesgo es que a veces se convierte en una discusión acerca de los costos.

¿Qué hay que hacer para proteger los datos correctamente? ¿Qué riesgo voy a correr si comparto parte de estos datos?

Y por supuesto, parte del debate de los costos creo yo que tiene que ver con estas conversaciones.

Uno de los problemas es que todo el mundo está evaluando el riesgo y lo que dice la ley. Y estas evaluaciones no son similares. Incluso dentro de los ccTLDs europeos, los RIRs, etc. vemos que toman diferentes decisiones sobre la base del asesoramiento que reciben y sobre la base de su apetito por riesgo.

Y la falta de predictibilidad es algo que estamos empezando a debatir y a entender lentamente, porque en última instancia queremos un sistema en el que haya seguridad en cuanto a que los datos son manejados adecuadamente por todos los involucrados, los que los recaban y los que los reciben y los usan.

Y ese es el punto de equilibrio al que tenemos que llegar. Porque, en última instancia, para la gente de ciberseguridad es importante usar los datos porque hay personas que tenemos que proteger. Y la ley dice que podemos tener ese acceso si lo pedimos de la forma adecuada. Y queremos ver cuál es la forma adecuada de lograrlo.

BRUCE TONKIN: ¿Quién más? Chris.

CHRIS LEWIS-EVANS: Gracias. En primer lugar, quisiera subrayar algunos avances que ya logramos en este grupo. Creo que la primera pregunta que usted hizo es muy buena, porque si hubiera hecho esa misma pregunta en la reunión de ICANN 61, creo que la respuesta del público habría sido muy diferente.

Creo que el cambio en la aceptación de lo que se necesita se debe a que diferentes partes de la comunidad van entendiendo cuáles son los diferentes requerimientos desde el punto de vista de la protección de datos y también desde el punto de vista de las partes que están autorizadas a tener acceso con fines lícitos, con un fundamento legal. Y esa comprensión proviene de entender los requerimientos de la gente.

En el EPDP se ha avanzado mucho cuando logramos entender cuáles son los requerimientos de las diferentes partes y las soluciones para satisfacer esos requerimientos.

Creo que esa es la mejor forma de entender bien cuáles son los requerimientos reales de todos y luego actuar sobre la base de esto. Realmente se trata de entender los requerimientos. Eso es lo que nos permite lograr una decisión equilibrada.

BRUCE TONKIN: Y ese es el propósito, ¿no? Ese es el propósito al que se refería Milton, cuál es el fin con el que recabamos los datos.

CHRIS LEWIS-EVANS: Para lograr una solución oportuna tenemos que centrarnos en esos requerimientos y equilibrar los requerimientos, entendiendo cuáles son las necesidades de todos.

BRUCE TONKIN: Si pensamos en los proyectos de TI, la razón número uno de que un proyecto de TI no funcione es porque no se dedicó el tiempo suficiente a establecer los requerimientos, así que creo que es un aspecto común y tenemos que hacer esto bien. Cristina.

CRISTINA MONTI: Gracias. Soy Cristina Monti, de la Comisión Europea. Repitiendo algunos de los comentarios que ya se hicieron.

Si miramos hacia adelante y hacia cuáles son los impedimentos, creo que es importante reconocer que estos temas existen desde hace mucho tiempo.

Y quizás hay algo que el GDPR logró y es plantear el tema y obligarnos a todos a buscar una solución en poco tiempo.

Y creo que ya se ha hecho mucho. Ya vimos en el público que hoy en día nadie piensa que la privacidad no es importante. Todos están de acuerdo en que los datos personales son algo valioso. Y aquellos que manejan datos personales deben ser responsables por el uso y el manejo de esos datos.

Y creo que incluso acá, en el entorno de la ICANN, se ha avanzado mucho en el sentido de que ahora, al menos, todos nuestros canales de comunicación están abiertos. El tema de la reforma de WHOIS

forma parte de la agenda en muchos debates de alto nivel, incluso fuera de la ICANN. Entonces creo que, en este sentido, se ha avanzado y los debates están pasando a una fase más madura.

Y ahora nos estamos centrando en las soluciones propiamente dichas. Y es acá en donde surgen las cuestiones reales. Por supuesto, en la operacionalización de los principios, es allí donde está dificultad. Y yo creo que si, en cierta forma, el modelo multisectorial que tenemos acá en la ICANN está demostrando ser difícil porque hay muchos intereses diferentes y a veces hay debates que están muy polarizados, yo creo realmente que únicamente será posible encontrar una solución disponible en este entorno multisectorial.

Además, creo que en este momento sabemos que se han tomado medidas para garantizar que el registro WHOIS cumpla con GDPR pero, una vez más, no llegamos todavía al punto en que tengamos una solución predecible y final.

Y esto, creo yo, tiene un impacto sobre muchos actores, como bien sabemos. Y a veces creo que no se presta atención al aspecto de que incluso los registradores individuales o los usuarios individuales no son conscientes de cómo se manejan los datos, con quién tienen que contactar si quieren corregir sus datos, etc.

Entonces, incluso desde esa perspectiva, estamos ahora en una situación en la que estaríamos en un punto intermedio.

BRUCE TONKIN: Sí, creo que lo que usted dice con respecto a los usuarios individuales es muy cierto. Porque mi experiencia indica que la mayoría de los usuarios individuales no saben qué es WHOIS. La mayoría de los que estamos acá somos profesionales en la industria de la TI o estuvimos antes en una reunión de la ICANN y lo escuchamos nombrar.

Pero el usuario promedio no piensa en usar WHOIS. El usuario promedio solo piensa que si tiene una mala experiencia con un sitio web lo va a denunciar al departamento de defensa del consumidor o a algún otro grupo, sin saber que estos servicios existen. Y no son conscientes de que su información se está publicando en algún lugar, entonces tenemos que lograr que esto sea más transparente. Esto es importante.

CRISTINA MONTI: Y para agregar algo al tema que se planteó sobre el riesgo, quisiera señalar que el GDPR, que se apoya en reglas que ya existen desde hace mucho tiempo, de hecho, debería ser entendido como un incentivo para que todos los actores que manejan datos personales lo hagan de una forma legal, responsable y transparente. Y creo que el GDPR ahora, incluso para los actores que están fuera de Europa, podrán ver que la situación mejor ahora, habrá más uniformidad en la forma en la que se aplican las reglas porque contamos con mecanismos para hacerlo ahora.

Entonces, antes del GDPR había muchas legislaciones nacionales diferentes, y ahora con GDPR tenemos una mayor uniformidad, incluso para los actores que están fuera de Europa ahora será mucho

más fácil resolver estos temas. Entonces quería señalar este punto también. Gracias.

BRUCE TONKIN: Sí, mejorar la estandarización es importante, sin duda.

HADIA ELMINIAWI: Tal y como se dijo antes, el desafío es un malentendido. Quisiera señalar rápidamente que nosotros no recabamos datos para dárselos a aquellos que tienen interés en acceder a los datos. Porque hay malentendidos.

Yo escuché que la gente dice, "Ustedes recaban datos para organismos de autoridad de la ley, para ciberdelito, para esos grupos". Y yo quiero asegurar a todos los que están acá que los datos se recaban únicamente con el fin de poder prestar el servicio.

BRUCE TONKIN: Que es el principio de minimización de los datos, es decir, identificar el propósito y recabar los datos que se necesitan.

HADIA ELMINIAWI: Y las terceras partes necesitan tener acceso a esos datos.

BRUCE TONKIN: Nick. No quiero tampoco que hablemos sobre un tema en particular, sino sobre el principio en general.

Nick.

NICK WENBAN-SMITH: Hay un riesgo, y el riesgo lo corren las partes contratadas. Esta es una de las cosas que nos hace tener una política más conservadora. Y esto nos lleva a un punto más amplio, porque yo personalmente no tengo miedo acerca de lo que dice [Inaudible], las penalizaciones financieras que podrían venir. Para ser organizaciones responsables, esta no es una preocupación seria.

A mí me preocupa mucho más en esta era de la ciudadanía digital la reputación de manejar los datos de manera legal, lícita y en función de la ley. Es una ventaja competitiva. Desde mi punto de vista, esa es una consideración importante, y me gustaría también incorporar esto en nuestro debate.

BRUCE TONKIN: Creo que a lo que se está refiriendo es a la confianza. Mucha gente pierde la confianza porque se brindaron sus datos para un servicio en particular. Y luego se enteran de que esos datos son entregados a una tercera parte y que son utilizados de una forma diferente.

Creo que, volviendo a las metas más generales de la ICANN, creo que necesitamos que la gente confíe en el sistema de nombres de dominio, que confíen en que pueden registrar un nombre de dominio y que confíen en que vamos a cuidar esos datos correctamente. De lo contrario, la gente que registra los nombres de dominio va a decir, “Para eso uso una red social”.

MILTON MUELLER: Yo quería volver a algo que dijo la Sra. Monti. Este es un tema muy general en relación con el rol de la ICANN como institución de gobernanza global y quiero hablar acerca de cómo esto se relaciona con los estados, los gobiernos y sus legislaciones. Porque este es uno de los temas clave de los que estamos hablando acá.

Yo no fui un gran fanático del Reglamento de Protección General de los Datos antes de GDPR. Pero debo admitir que, mirando hacia atrás, creo que le hicieron un favor al mundo al establecer un estándar.

Entonces, en los campos regulatorios y de gobernanza tenemos algo que se llama "el efecto California". Cuando el estado de California estableció estándares de contaminación para los vehículos, eran muchos más estrictos que los que había en el resto del país. Y los fabricantes tuvieron que decidir entre fabricar un coche para California y un coche diferente para las otras jurisdicciones, o fabricar un solo vehículo. Y básicamente eso es lo que va a pasar ahora con GDPR y la privacidad. Establecieron un estándar. Y yo creo, como agencia global, la ICANN puede cumplir con este estándar o tener un estándar que compite.

Por ejemplo, si Estados Unidos decide que no le gusta lo que hizo Europa, puede establecer un estándar diferente y en ese caso vamos a tener un sistema más conflictivo. Este es uno de los grandes temas de los que tenemos que ser conscientes al hablar acerca del cumplimiento del GDPR.

Y utilizo Estados Unidos como ejemplo, pero cualquier otra gran jurisdicción podría crear los mimos problemas. Podría ser China, la India o quizá Canadá. No sé.

Pero, ¿entienden a lo que me refiero? Hay un tema acá muy importante que tiene que ver con el estado de la ICANN como un organismo de gobernanza global del sector privado, a diferencia de la soberanía territorial fragmentada, en donde podríamos tener múltiples sistemas coexistiendo.

BRUCE TONKIN: Y creo que, si vemos la historia de GDPR, esto es lo que pasó en Europa, en los diferentes países. Los distintos países tomaban los principios, pero los interpretaban de manera diferente, y esto implica un costo para las empresas. Yo me imagino que una empresa que apunte a un mercado grande en Alemania. Una empresa que quiera apuntar a otro mercado, pero no lo va a intentar porque las leyes de privacidad son muy complicadas. Entonces creo que, al unificar todo esto, la gente puede ver un gran mercado, al igual que en el caso de California. Y quizás había otro estado en Estados Unidos que tenía una población pequeña, pero California es una economía muy grande. Y de esta forma, los fabricantes de automóviles van a fabricar vehículos para ese mercado que los otros mercados también van a poder aprovechar.

FLIP PETILLION: Gracias, Bruce. Quería agregar algo con respecto a la confianza.

Tiene que haber confianza cuando uno da información, pero también cuando uno solicita información. Todo el mundo debería mostrar su compromiso de contribuir a esa confianza. Y creo que Nominet dio un buen ejemplo. También vimos otro ejemplo con el Sr. Noss, sobre un registrador en particular. Y estos son buenos ejemplos de compromiso, de buena voluntad. En Europa diríamos de buena fe. Es la voluntad de encontrar una solución que funcione. Quería mencionar esto.

BRUCE TONKIN: Uno de los puntos clave en cuanto al acceso a los datos es que cuando una parte solicita acceso, después de obtener los datos se vuelve responsable de esos datos y de lo que pasa con esos datos. Entonces no se trata solamente de acceder a los datos y ya está, no es que pueda hacer lo que quiera con esos datos, esa responsabilidad debe formar parte de este marco de confianza. Aquellos que tienen acceso a los datos y no los usan de forma adecuada, pierden el acceso a los datos. Así de simple.

Ahora quisiera ver si algún miembro de algún público quiere hacer algún comentario. Tengo otras preguntas para el panel, pero considerando que acá tenemos a diferentes miembros de la comunidad, quisiera abrir el espacio para que el público haga preguntas al panel, especialmente en relación a este tema. ¿Cómo logramos llegar a una solución oportuna? ¿Cómo llegamos todos juntos a esta solución?

No veo ninguna pregunta. A ver, aquí si hay una pregunta.

HOLLY RAICHE: En términos de propósito, tenemos que someter a prueba el propósito en términos de ICANN. Yo sé que el alcance de ICANN es bastante amplio. Yo escuché argumentos que dicen este ámbito o que este alcance solo tiene que ver con las cuestiones técnicas. Pero yo creo que no estamos hablando solamente de la parte técnica, estamos hablando de resolución de disputas. Y cuando hablamos de propósito, a mí me preocuparía que la misión sea el manejo del sistema general y su estabilidad.

BRUCE TONKIN: ¿Alguien quiere hacer algún comentario?

ASHLEY HEINEMAN: El EPDP llegó para conocer esto. En cuanto a desarrollar el propósito, creo que capturamos todo lo que usted mencionó, y eso es algo bueno. No terminamos todavía, pero se reconoce esto, especialmente con respecto a la seguridad, estabilidad y flexibilidad del Sistema de Nombres de Dominio.

BRUCE TONKIN: ¿Hay otra pregunta? Número uno.

ORADOR NO IDENTIFICADO: Yo soy número uno.

RACHEL POLLACK: Rachel Pollack, de UNESO. Gracias por este debate tan interesante.

Dos comentarios rápidos y una pregunta. En la última reunión de la ICANN a la que asistí en Copenhague, hace un año y medio aproximadamente, el Consejo de Europa llevó a miembros del comisionado de protección de los datos para facilitar el debate entre los comisionados de protección de los datos y miembros de la comisión de la ICANN, y fue muy interesante. Hay una especie de eco -- Entiendo que publicaron una guía a principios de este año acerca del tema de la protección de los datos dentro de la ICANN. Entonces, me preguntaba si algún miembro del panel había visto la guía, qué opina, si prevé que volveremos estos debates con los comisionados de protección de los datos para asegurarnos de que el modelo que se adopte en última instancia tenga una estructura y esté estructurado de manera sistemática.

En términos de mi propia organización, esto no está directamente relacionado con la ICANN, pero quisiera decir que nosotros publicamos dos estudios que analizan las cuestiones de libertad de expresión, privacidad y transparencia. Y también habla acerca del equilibrio entre los derechos humanos y cómo alcanzar este equilibrio. Así que quisiera recomendarles que lean la serie sobre libertades en Internet de la UNESCO.

BRUCE TONKIN: Yo hablé con los comisionados de protección de los datos y los invité a que participaran en este evento, pero tenían un evento en paralelo esta semana. Entonces, lamentablemente, no pudieron participar.

Pero para responder la pregunta – sí, Hadia.

HADIA ELMINIAWI: En respuesta a su pregunta, nosotros sin duda consideramos todas las correspondencias con la Junta de Protección de Datos Europea y todos los asesoramientos brindados a la ICANN. Durante este trabajo y al desarrollar la política, consideramos todo lo que se nos brindó.

BRUCE TONKIN: Cristina.

CRISTINA MONTI: Quizá para aclarar y complementar la pregunta. Por supuesto, conocemos la guía que brindó el Consejo de Europa, que es un documento útil; sin embargo, se ocupa de los principios. Y aquí estamos trabajando con el GDPR, y el Consejo de Europa está más bien a cargo de la Convención 108, que es un instrumento diferente. Y debemos recordar esto.

Con respecto a las autoridades de protección de datos, usted tiene razón, podrían haber venido a esta reunión o no podrían haber venido a esta reunión porque hay una importante reunión internacional celebrándose en este momento en Bruselas, pero también quisiera garantizarles y darles la certeza de que las autoridades europeas de protección de datos conocen estos debates e intercambios de ideas, los están siguiendo y están viendo el avance que se ha logrado, y han brindado guía y orientación cuando se les pidió que hicieran

comentarios específicos, y creo que están predispuestos a continuar con este intercambio de ideas. Y esto tiene que ver con lo que se dijo acerca de los temores a las multas.

Sí, las autoridades de protección de datos tienen mayores poderes, pero tienen muchas herramientas a su disposición. Entonces, antes de aplicar una multa, supongo que utilizarían las otras herramientas que tienen, por ejemplo, enviar una advertencia o una notificación. Y, por lo tanto, creo que están demostrando también buena predisposición al diálogo en este sentido. Y creo que eso es muy importante.

BRUCE TONKIN: Sí, creo que ese es un punto muy valioso. El punto de inicio del cumplimiento y la aplicación en la legislación es un abordaje conjunto que permite a todo el mundo entender cuáles son los requerimientos. Y en realidad solamente si se ignoran se aplican las multas.

ORADOR NO IDENTIFICADO: Tenemos una pregunta de un participante remoto para Nick. “La experiencia de las partes contratadas respecto al acceso es muy valiosa. ¿Qué cantidad de pedidos de acceso a información por parte de terceros ha recibido Nominet que no proviniera de autoridades de aplicación de la ley? ¿El CPH está pensando publicar esta información?”

NICK WENBAN-SMITH: Este es un abordaje más empírico al desarrollo de políticas y habría que ver cuál es la experiencia.

Siempre tuvimos una política de acceso a los datos, aun antes del GDPR teníamos algunos elementos de datos que no publicábamos en el WHOIS. Estamos hablando del código país .UK, que es uno de los códigos de país más importantes. Tenemos 12 millones de dominios, y hemos visto un aumento en las solicitudes de datos.

Antes del 25 de mayo no publicábamos las direcciones de correo electrónico ni los teléfonos en el WHOIS público. Había que pedirlos a través de un proceso especial que existía desde hace tiempo. Después del GDPR, estamos recolectando la información y yo analizo esta información muy cuidadosamente, dado que me interesa mucho. Hemos recibido casi 800 solicitudes en relación con datos de registración de los nombres de dominio en tres meses. Y vamos a considerar los seis meses posteriores al 25 de mayo para ver qué pasó, cuántos informes se solicitaron, etc.

Pero cuando recibimos una solicitud, obviamente la analizamos e informamos al sujeto de los datos que estos datos fueron solicitados y, si está de acuerdo, los brindamos.

Hay diferentes sistemas de información y de informes relacionados con cada pedido individual, pero, sí, de aquí a futuro vamos a encararlo dentro de la organización. Y en el grupo de partes contratadas se ha hablado mucho de estos temas, de cómo estamos recabando toda la información y estamos tratando de usarla junta y ver la experiencia diferente y ver qué funciona y qué no. Los números

no han sido tan importantes en cuanto a solicitudes de datos. Y esto se debe en parte a que brindamos muchos datos a las autoridades de aplicación de la ley en nuestro país sin necesidad de hacer pedidos individuales. Y estoy un poco nervioso, y yo sé que la solución RDAP está allí para brindar acceso, y las partes contratadas apoyan esto, pero me preocupa por experiencias anteriores y por la forma en que la ICANN ha implementado cosas en el pasado, que terminemos teniendo una implementación muy compleja y costosa que sea mucho más grande de lo que realmente necesitamos, considerando la cantidad de pedidos que se recibe. Por supuesto, .UK es un registro muy importante, son diferentes los dominios que tienen que ver con Gales, donde hay muchos menos dominios y se reciben muchos pedidos allí.

En cuanto al programa de los nuevos gTLDs, bueno, esto explica lo que pasa en muchos gTLDs más pequeños. Hay muchos casos diferentes y en algunos casos hay registros pequeños con costos muy altos que no justificarían la escala y el costo de la implementación. Yo quisiera saber, entre registros más pequeños, si realmente recibieron alguna solicitud de información.

BRUCE TONKIN: La pregunta, dejando de lado las autoridades de la ley, y si escuché correctamente, ¿reciben 800 pedidos en tres meses?

Micrófono 1, tiene que conseguirse un número usted.

ORADOR NO IDENTIFICADO: Gracias, Bruce. Quiero preguntar algo porque usted dijo algo con respecto a uno de los principios del GDPR sobre la exactitud, y usted dijo que aproximadamente es un tema casi resuelto porque hay normas de exactitud que exigen que se actualice una vez la información de los registratarios en WHOIS. Y este es un debate continuo en el proceso del EPDP, yo creo que esto no es muy diferente de una buena solución, no estamos lejos de esto, porque la pregunta es, ¿cómo podemos cumplir el objetivo si tenemos información no exacta o falsa? ¿Cómo podemos cumplir ese objetivo? Y no lo pregunto solo desde el punto de vista de terceros que quieren esta información, sino también para las partes contratadas o la ICANN o quien sea que busque esta información, por ejemplo, para ponerse en contacto con alguien y se dan cuenta de que los datos no son exactos o son obsoletos, o lo que fuera.

Creo que este es un tema que estamos dejando de lado, bajo la alfombra. Yo sé que hay muchos costos involucrados aquí, que es un problema tedioso, pero no creo que hayamos llegado a una solución satisfactoria hasta ahora.

BRUCE TONKIN: Estamos hablando de la autenticación de los datos.

¿Hay algún comentario? Milton.

MILTON MUELLER: Creo que el fantasma del antiguo WHOIS todavía está preocupando a muchas personas. Y el tema de la exactitud es un ejemplo de esto.

Hemos tenido acceso indiscriminado a datos personales, y tanto los buenos actores como los malos actores, por razones obvias, ingresan datos inexactos en WHOIS porque saben que van a ser publicados. Una vez que estos datos empiecen a estar protegidos del acceso indiscriminado, entonces el problema de exactitud es un problema totalmente diferente. Sí, habrá personas que ingresen información falsa, pero la mayoría de los usuarios o registratarios legítimos no lo harán.

Además, este debate en cuanto a la verificación de los datos es un problema octogonal, que tiene que ver con los principios de por qué recabamos información y para qué. Esto tiene que ver con una política diferente, con un problema de exactitud.

Y este es un buen ejemplo de los obstáculos para el progreso, porque se empieza a agregar cosas al proceso, de decidir qué recabamos y cómo cumplimos con GDPR. En realidad, es un problema octogonal que tiene que ver con el cumplimiento de GDPR. Y esto puede resolverse a través de otros procesos más adelante.

BRUCE TONKIN: Número dos.

FIRDAUSI: Gracias. Yo soy Firdausi.

Quisiera hacer una pregunta acerca de los conflictos. Quisiera ver qué tiene que ver esta regulación, si es una regulación específica que

modifica la general o si es una regulación nueva que elimina la antigua.

Quizás habría que ver si hay un objetivo para las investigaciones. Si consideramos GDPR, por ejemplo, quisiera saber cómo puede implementarse este principio legal general, o quizás haya una teoría que pueda implementarse. Y, además, porque considerando que el GDPR se aplica no solamente en la Unión Europea sino también en el resto del mundo, entonces, en la práctica, ¿cómo harán los gobiernos de otras regiones que tienen instituciones similares? Por ejemplo, en el sudeste asiático hay una organización similar, y cómo harán estos países para cumplir con el GDPR. ¿Quizás a través de tratados multilaterales o bilaterales o a través de un acuerdo de asistencia mutua individual de cada país?

También escuché que los panelistas hablaron acerca de tener en cuenta la privacidad, que los consumidores tienen que conocer todo esto y también cuál es la función de los funcionarios de protección de datos o funcionarios de privacidad en este contexto. Porque esto significa que, aparentemente, la Unión Europea a través del GDPR está estableciendo una obligación para muchas empresas del mundo de tener un funcionario de privacidad o de protección de datos.

BRUCE TONKIN: Tengo algunas respuestas, pero primero voy a preguntar a Nick si recibió pedidos de información de personas o partes de fuera del Reino Unido y cómo trataron estos pedidos de información.

NICK WENBAN-SMITH: Sí, tenemos un proceso estándar. No importa de dónde proviene el pedido. Recibimos pedidos de fuera del Reino Unido. La mayoría de los pedidos provienen del Reino Unido, y creo que esto se debe que la mayor parte de las registraciones están en este país y porque esa es nuestra situación legal. Tenemos las mejores redes, pero tenemos muchos registradores fuera del Reino Unido, y muchos registratarios fuera del Reino Unido. Y se aplica la misma política, porque es una política global.

Y creo que cuando consideramos cómo funciona GDPR en la práctica, es interesante ver que se está logrando mucha estandarización en la forma en que creamos nuestro trabajo.

Entonces no importa de dónde venga la solicitud.

BRUCE TONKIN: Como ustedes están en Europa, están obligados por la legislación europea, entonces básicamente aplican esa legislación a cualquier solicitud de información que reciban de cualquier parte del mundo.

NICK WENBAN-SMITH: Pero en cuanto a la implementación y al acceso, es la misma política para todos. No es obligatorio, pero es más simple para nosotros hacerlo así.

BRUCE TONKIN: Tiene una respuesta a un proceso estandarizado.

Ashley, quizá podría hablar en nombre de un gobierno diferente, un gobierno que no esté en Europa. Ustedes consideran que quizá los registros y registradores deben tomar en cuenta otra legislación diferente al GDPR.

ASHLEY HEINEMAN: Yo no voy a hablar en nombre de los Estados Unidos porque no puedo hacerlo. Voy a hablar en nombre del GAC. Estoy aquí en nombre del GAC. Pero quiero decir que debemos tener cuidado cuando decimos que el GDPR es un estándar para la protección de datos y la privacidad global. Hay muchas normas de protección de datos en el mundo, y creo que lo que trajo esto como tema para la ICANN es el tema de la responsabilidad para las partes contratadas que todo esto implica.

Entonces, esperamos que gran parte de lo que incluye el GDPR esté dentro del mismo régimen de otras leyes de protección de datos, pero también tenemos el conflicto con procedimientos legales locales, y habría que ver cómo juega todo esto. Pero creo que para los gobiernos es importante, en cuanto a la implementación de todo esto, la capacidad de las autoridades de aplicación de la ley fuera de la Comisión Europea, porque está claro que el GDPR permite una justificación al acceso más sencilla para las autoridades europeas de aplicación de la ley. No está tan claro que se aplique a otros organismos de aplicación de la ley fuera de Europa.

Gracias.

BRUCE TONKIN: Gracias.

Número uno.

ORADOR NO IDENTIFICADO: Yo soy [Janis Sordie]. Tengo una pregunta acerca de su comentario cuando usted dijo que reciben 800 solicitudes en tres meses.

Antes del GDPR, ¿cuántas solicitudes recibían de forma mensual? Quizá conocen las cifras de los últimos años, porque esos serían datos más interesantes, conocer la cantidad de solicitudes que se recibe en general.

NICK WENBAN-SMITH: Gracias por la pregunta. No es exactamente la misma cifra mes tras mes, porque a veces se recibe un pedido importante de un organismo en particular. Por ejemplo, en las fechas anteriores a Navidad, o que quizás haya una investigación más importante.

Creo que la escala del cambio en el número de solicitudes pasó de 10 a 20 por mes, alrededor de 250 por mes. Esa es la escala del cambio.

BRUCE TONKIN: ¿Se publicaron ampliamente sus servicios y lo que pasó con el GDPR en Reino Unido? ¿Hay una mayor concienciación?

NICK WENBAN-SMITH: Es una pregunta interesante, porque lo más importante con respecto al GDPR es que no cambió la legislación en el Reino Unido, pero lo que sí pasó es que ahora todas las personas conocen sus derechos como ciudadanos. Tienen un enorme conocimiento sobre sus derechos, porque el sitio web de la BBC publicó mucho sobre este tema antes del 25 de mayo, y el 25 de mayo ocupó los titulares de todos los medios en el Reino Unido.

BRUCE TONKIN: O sea, hay más conciencia entre los consumidores.

Greg.

GREG AARON: Entonces, desde que se implementó GDPR en mayo, empezamos a entender lentamente las consecuencias y estamos empezando a ver que surge información acerca del uso y las solicitudes.

Recientemente, dos organizaciones integradas por profesionales en ciberseguridad y operadores de redes, empezaron a trabajar juntos con el grupo anti phishing y sus miembros incluyen empresas de seguridad que protegen redes, bancos, instituciones educativas, etc.

Y les preguntamos a los miembros: ¿Están presentando más solicitudes? ¿Qué pasa? Y había unas 300 personas que respondieron y brindaron información. Y lo que nos dijeron es que algunos de ellos ya no saben cómo solicitar la información. En parte porque las organizaciones que tienen los datos trabajan de manera diferente,

tienen procedimientos distintos, con diferentes mecanismos. Y esto los ha disuadido de presentar solicitudes.

Entonces la cantidad de solicitudes es limitada, quizás esto hable o no acerca de la demanda respecto de estos datos, porque algunas organizaciones decidieron dejar de usar datos de WHOIS a través del mecanismo disponible actualmente porque ya no reciben la información que necesitan. Creo que en los próximos meses sabremos mucho más sobre la forma en que esto ha afectado a las diferentes personas.

BRUCE TONKIN: Gracias.

Número tres.

DIRK KRISCHENOWSKI: Hola, yo soy Dirk Krischenowski, de .BERLIN y .HAMBURGO, y Vicepresidente del Grupo de Dominios de Alto Nivel de la Unión Europea.

En nuestro sitio web hemos estado publicando un estudio de 39 TLDs geográficos, así que preguntamos a los pequeños registros cómo se manejaron en términos del GDPR. Y de esos 39, había 25 TLDs geográficos y el resto eran no europeos. Y los resultados de esta encuesta fueron los siguientes. Los TLDs geográficos basados en Europa se toman muy en serio el GDPR y han implementado medidas

para proteger a los ciudadanos y su información personal, la cantidad de pedidos es muy pequeña y se resuelve de manera eficiente.

El estudio de los registros de TLD geográficos muestra que no hay una necesidad de un modelo de acceso universal en cuanto a cómo opera el GDPR en la práctica. Consideren este estudio. Es muy interesante. Identifica la cantidad de solicitudes recibidas, y entre mayo y septiembre la cantidad de solicitudes fue menos de 50 en los 39 TLDs geográficos que tienen más de 700,000 nombres de dominio registrados.

BRUCE TONKIN: Gracias, Dirk. Es muy interesante que se compartan datos. Creo que todos deberían hacer, todos los que manejan registros. Es muy bueno que compartan los datos como hizo Dirk, porque esto ayuda al desarrollo de políticas.

JOHN LAPRISE: Hola, John Laprise, de ALAC. Y ahora me voy a sacar mi remera de ALAC y me voy a poner la remera de mi trabajo diario. Yo trabajo en investigación de mercado, en un departamento de marketing de Estados Unidos. Y Bruce antes respondió una pregunta acerca de los efectos sobre Estados Unidos.

Hace poco asistí a un seminario web por trabajo. Muchas empresas en Estados Unidos son conscientes del GDPR y menos de la mitad están avanzando hacia la adopción. Están tomando una actitud de “esperar y ver qué pasa”. Nosotros tenemos la expresión de, “No hay que correr

más rápido que una pantera, sino más rápido que los demás". Esa es la posición que están tomando muchas empresas en Estados Unidos.

Pero la investigación de mercado en general y toda la industria está bastante involucrada en esto. Hay mucho trabajo en curso en ese sentido.

BRUCE TONKIN: Gracias por su aporte.

Dos.

THOMAS DE HAAN: Quisiera hablar acerca de lo que dijo el representante de Nominet. Creo que es muy útil ver cuáles son los mecanismos actuales que ya están implementados. Por supuesto, eso es dentro de la jurisdicción del Reino Unido, entonces es un poco menos complejo que lo que ocurre a nivel mundial.

Pero mi pregunta es: usted se refirió a solicitudes individuales de acceso a los datos. ¿Qué ocurre con acceso masivo? Por ejemplo, en Holanda tenemos uno de los ccTLDs más grandes del mundo, ellos llegaron a un acuerdo con las autoridades locales para tener un acceso masivo limitado. Ellos quizá lo puedan explicar.

Pero, ¿esto ocurre también en el Reino Unido? Y la pregunta básicamente se remite a lo siguiente: ¿los instrumentos que tenemos satisfacen esa demanda?

BRUCE TONKIN: Quisiera intervenir brevemente para aclarar algo en relación a la terminología. ¿"Masivo" es cuando toda la base de datos se da a un tercero? Y ese tercero puede hacer consultas. Creo que hay una diferencia, pero le voy a dar la palabra a Nick. ¿Ustedes brinda acceso masivo a los datos? Es decir, ¿le dan una copia completa de su base de datos a las autoridades de aplicación de la ley? ¿Tienen acceso automatizado? Y, en ese caso, ¿qué tipo de consultas se hace?

NICK WENBAN-SMITH: Gracias por la pregunta.

En cuanto al acceso masivo, nosotros permitimos que los organismos de seguridad el Reino Unido tengan acceso masivo. Pero tenemos aclarar de qué acceso estamos hablando, porque no es toda la base de datos.

El registro tiene muchos más datos de los que compartimos con las autoridades de aplicación de la ley. Y hay datos también el WHOIS público. Entonces hay distintos niveles. Pero, sin duda, el acuerdo al que llegamos con las autoridades de aplicación de la ley en nuestro país es que van a tener acceso exactamente a los mismos datos de WHOIS que estaban a disposición del público antes de mayo, pero lo van a hacer con un registro seguro, con verificaciones, individualizado. Nosotros tenemos una agencia de delito internacional, ellos coordinan todo eso.

Pero en cuanto a los estándares locales, esto se hace con un único punto de acceso a través de una única autoridad.

BRUCE TONKIN: ¿Y acceso automatizado?

NICK WENBAN-SMITH: No tenemos acceso automatizado.

BRUCE TONKIN: Milton.

MILTON MUELLER: Creo que el tema del debat ees un tema interesante, pero quiero subrayar que estamos hablando de acceso.

Entonces, en primer lugar, tenemos muchos datos interesantes que se recaban acerca de lso efectos reales. La información de gTLD es muy interesante. Después la encuesta de ccTLDs. Es muy bueno lo que dijo Greg acerca de la investigación sobre seguridad.

Y creo que estamos viendo cuán complejo es todo. En Nominet se hablaba acerca de los diferentes niveles y tipos de acceso. Este tema puede llegar a ser muy complejo, como podrán ver.

Dirk que no necesitamos acceso unificado. Y hay una justificación razonable para decir que sí lo necesitamos. Este es un tema con el que tenemos que lidiar.

Pero, en primer lugar, tenemos que decidir qué tenemos en el WHOIS, qué es lo que se publica, cuáles son elementos de datos que se recaban. Y, por favor, no confundamos esos temas.

Y deberíamos poder finalizar la primera parte. Creo que es relativamente fácil en tres meses. Y si no lo podemos hacer en tres meses, tenemos un gran problema, porque los plazos de la política se van agotando y todo el proceso multisectorial va a parecer un fracaso. Y, como dije antes, hay aves de presa que están circulando cerca y que les gustaría que nosotros fracasáramos y que les gustaría entrar y hacer intervenciones a nivel gubernamental.

Entonces, como dije antes, primero resolvamos el tema de las especificaciones temporarias y formalicémoslo como política y luego tengamos un debate rico acerca del acceso.

BRUCE TONKIN: Sí, una de las cosas desde el punto de vista del desarrollo de software es, primero, hacer el desarrollo de software para tener algo y después trabajar sobre eso.

Tenemos que ver en cierta medida si en este caso es lo mismo, cuáles son los datos que estamos recabando y cuáles son los datos que se entregan.

Número tres.

BECKY BURR: Hola, soy Becky Burr, y hablo como Directora de Privacidad.

Quería hablar acerca de lo que dijeron sobre las empresas norteamericanas. Creo que muchas empresas vieron que Microsoft, cuando lanzó su plataforma GDPR para pedidos de datos, la lanzó a nivel global. Y ahora ya informaron que a nivel por cápita y absoluta están recibiendo más solicitudes de norteamericanos que de ningún otro lugar del otro mundo. Esta es la experiencia que tenemos con el sistema norteamericano.

Y coincide con nuestra experiencia el hecho de que Europa era consciente del GDPR el 25 de mayo, también se sintió en todo el mundo. Esta empresa norteamericana y otras empresas con las que yo trabajo están también cumpliendo con GDPR y avanzando rápidamente como forma de responder a las demandas de los consumidores.

BRUCE TONKIN: Gracias, Becky.

Número uno.

AMRITA CHOUDHURY: Hola, yo soy Amrita Choudhury, de CCOUI, la India.

Quizás este equivocada en lo que digo, pero corríjanme si me equivoco. Creo que hay aproximadamente 339 millones de nombres de dominio registrados. Y hay aproximadamente 12 que caen bajo el dominio de la Unión Europea. Esto es menos de la cantidad de dominios registrados.

Si bien se habla mucho en la ICANN acerca de cómo los nombres de dominio pueden cumplir con GDPR en términos del registro de WHOIS, ¿la ICANN también está considerando las legislaciones de otros países? Europa es una zona. Pero hay otras regiones. ¿Los intereses de esas regiones también se están protegiendo?

En segundo lugar, hay países muy desarrollados, que entienden muy bien la situación; y hay otros países que son emergentes, por ejemplo, la India, donde tenemos nombres de dominio que son vendidos por diferentes empresas de Europa, Estados Unidos e incluso la India. Los registros y los registradores quizá no tengan los mismos conocimientos y capacidades.

Entonces se está planificando algo en cuanto a desarrollar estos conocimientos para que los consumidores finales también puedan ver sus intereses protegidos porque hablamos, pero los nuevos usuarios de Internet o los compradores de nombres de dominio no son conscientes de esto, especialmente los países emergentes.

BRUCE TONKIN: Creo que hizo tres preguntas en una. Por un lado, ¿cómo están considerando las legislaciones de otros países? Obviamente, hay legislación en la India.

La segunda pregunta es, ¿cómo se genera conciencia entre la gente de distintas partes del mundo con respecto a estos temas?

Vamos a pedirle a Hadia, de ALAC, que responda primero a la segunda pregunta. Supongo que ALAC está haciendo cosas para generar conciencia en distintas partes del mundo.

HADIA ELMINIAWI: Voy a hablar como miembro del EPDP. Una de las recomendaciones que salió del equipo de EPDP es hacer recomendaciones para generar concienciación entre los registratarios.

Y yo creo que esto en parte lo puede hacer la ICANN y en parte también los registros y los registradores, porque creo también que a los registradores les conviene que los registratarios sepan lo que pasó y cuáles son las nuevas políticas.

¿En nuestro trabajo estamos considerando otras legislaciones de privacidad? La respuesta es no, porque el equipo de EPDP tiene por fin ver el cumplimiento de las especificaciones temporarias con GDPR. Esperamos que no haya conflictos con otras legislaciones de privacidad.

Pero en este momento no estamos haciendo este trabajo. Es decir, no estamos considerando otras leyes de privacidad.

BRUCE TONKIN: Gracias. Ashley.

ASHLEY HEINEMAN: Voy a hablar en nombre del GAC. Sí, en términos de nuestra participación en el EPDP y en otras actividades relacionadas con WHOIS, nosotros tratamos de hacer todo lo posible por reconocer que hay otras leyes de protección de datos en el mundo. Tratamos de hacerlo utilizando GDPR como base, pero estamos tratando de que no sea todo específico en función de GDPR. Hacemos lo posible por respetar todas las legislaciones de todo el mundo. Pero eso es lo que estamos tratando de hacer.

BRUCE TONKIN: Gracias. Cristina.

CRISTINA MONTI: Yo también quería hacer algunos comentarios sobre estos temas recurrentes acerca de la tensión potencial entre diferentes legislaciones, diferentes jurisdicciones y la naturaleza global de Internet. Sabemos que este es un desafío con el que nos vamos a seguir enfrentando, no solamente en relación con la protección de datos sino también otras áreas, y por eso es tan importante hacer las cosas bien acá en la ICANN, porque este será un caso de prueba para el futuro.

En cuanto a la protección de datos, en términos generales quisiera subrayar también que lo que vemos, y quizás yo soy más optimista que mi colega Milton Mueller, es que hay una tendencia hacia la convergencia. Los principios que forman parte del GDPR y que forman parte de los derechos humanos fundamentales son principios, diría

yo, de sentido común. Tienen que ver con hacer una buena gestión de los datos.

Tal y como dijeron al principio, el diablo está en los detalles y en la implementación. Es allí a donde tenemos que volcar nuestra atención.

Podría ocurrir que no todas las respuestas estén allí. Y quizá descubramos que necesitamos también llegar a una solución creativa para que el sistema funcione. Quizá tengamos que ir más allá de los límites actuales. Por eso tenemos procesos, tenemos a las múltiples partes interesadas sentadas en la mesa y deberíamos lograr que funcione.

Mi opinión con respecto a los diferentes procesos es que yo entiendo que hay algunas partes interesadas que quisieran tener un abordaje secuencial, mientras que otros tienen esta sensación de urgencia y quieren llegar a una solución final.

Yo personalmente no creo que haya problemas en cuanto a tener procesos paralelos, pero está claro que es necesario entender muy bien cuáles son las cuestiones. Y a veces hay malentendidos que vuelven a aparecer una y otra vez.

Y, por lo tanto, es sumamente importante prestar atención a lo que los otros están diciendo, en los diferentes grupos de trabajo, todos colectivamente trabajamos para alcanzar una solución.

Y si hay algún tema que no se pueda resolver, entonces identifiquemos juntos cómo vamos a trabajar para cerrar esa brecha. Gracias.

BRUCE TONKIN: Gracias, Cristina.

Quisiera pasar a otra pregunta y después voy a volver al público. Es otra pregunta para el panel.

Desde el punto de vista del desarrollo de políticas, en los últimos años se desarrollaron otras políticas relacionadas con este tema.

Una de ellas es la solución que implementaron los registros y los registradores para proteger los datos personales y la privacidad, y esta fue la introducción de lo que a veces se llama servicios de privacidad o servicios de representación.

Pero es acá en donde se reemplaza información que está en WHOIS de otra empresa, en este caso de representación o puede ser el nombre de la dirección del registrador en lugar del nombre y dirección del registratario. Y básicamente operan con un servicio que reenvía, es decir, si se envía un correo a una dirección que está en WHOIS, esa dirección luego se reenvía al usuario final.

Entonces, se trata de dar a los consumidores la opción de proteger sus datos personales, pero lo que no quedaba claro era bajo qué circunstancias se divulgaban luego los datos personales a las autoridades de aplicación de la ley y cómo pueden acceder a estos datos las autoridades de aplicación de la ley y otros grupos.

Entonces hubo un proceso de desarrollo de política sobre este tema. Pero ahora que estamos hablando de este nuevo tema, la pregunta

para el panel es, ¿deberíamos revisar estas políticas? ¿Deberíamos considerar estas políticas cuando desarrollamos nuevas políticas en el EPDP?

El otro tema tiene que ver con el concepto del WHOIS extenso. Algunos de los registros .COM tienen información sobre el nombre de dominio, información del DNS, información sobre el registrador. Y luego hay que ir y pedir al registrador información sobre el titular del nombre registrado. Es un sistema distribuido. Entonces, hace unos años, se pensaba que era difícil tener diferentes sistemas porque el formato de los datos era diferente en todos los casos. Y en ese momento, entonces se utilizaba el puerto 43 de WHOIS. Entonces el proceso de desarrollo de políticas decía que teníamos que tener toda la información en un registro central para poder hacer la búsqueda en un solo lugar. Pero lo que está pasando ahora es que hay reglamentaciones, diferentes países, que hay restricciones con respecto a la transferencia de datos entre países. Y al parecer hoy en día la posición es que, si tenemos un registrador en Australia y tenemos clientes australianos, entonces mantenemos los datos en Australia. Si estamos operando un registro en Alemania, en Irlanda o en otro país, entonces se conservan los datos de los clientes en el país donde están los clientes y esos datos no se divulgan.

La pregunta para el panel es la siguiente, considerando que tenemos estas tres políticas que ya existen, podrían entrar en conflicto con el trabajo que está haciendo el EPDP, y yo escuché que el panel habló acerca de cómo consideramos el trabajo que se hizo hasta ahora y que tenemos que actualizarlo y, quizá, buscar otros abordajes. ¿Ashley?

ASHLEY HEINAMN: Voy a ser muy breve porque quizá mis colegas de aplicación de la ley puedan responder mejor a esta pregunta. Pero yo quiero hablar acerca del equipo de revisión de privacidad y representación. El trabajo de este equipo tuvo un gran impacto. Las cosas están bastante detenidas por el momento. Ahí me preocupa especialmente aquellos que quieren obtener acceso a esta información, que no puedan acceder cuando sea necesario, porque estamos ingresando en el mundo de GDPR, y necesitamos contar con herramientas para poder hacer esto. Entonces tenemos que lograr que el trabajo tenga un impacto, pero no que detenga el trabajo de implementación.

BRUCE TONKIN: Gracias, Ashley. ¿Alguien más?

MILTON MUELLER: No quiero hablar sobre privacidad y representación sino sobre el WHOIS extenso. Por lo que yo sé, el WHOIS extenso ya no será necesario en virtud del GDPR una vez que hayamos implementado RDAP. La necesidad del WHOIS extenso se verá superada por RDAP, y no habría un fundamento para que los datos sean conservados en el registro.

BRUCE TONKIN: ¿Podría explicar un poco más esto?

MILTON MUELLER: Tendríamos una especie de base de datos federada y la gente que quiere acceso a los datos podría tener acceso sin tener que almacenarlo en dos lugares diferentes, el registro y el registrador. Eso es por lo que yo entiendo. Podría estar equivocado. Y creo que el fundamento para el WHOIS extenso era que facilitaba la transferencia de dominios de diferentes registradores a otros, pero creo que ahora deberíamos poder hacer esto sin tener el WHOIS extenso. Y en línea con GDPR, el principio de minimizar la transferencia y recopilación de datos indicaría que los datos deberían estar en el registrador, que es el que recaba la información.

BRUCE TONKIN: Muy bien. Greg.

GREG AARON: Una de las cosas que vimos en nuestra experiencia en los últimos meses en relación con la especificación temporaria es que, si bien GDPR cubre determinadas clases de datos, las especificaciones temporarias permiten la reducción de datos adicionales que no están cubiertos por la ley. Por ejemplo, GDPR no cubre la información de lo que se llaman las personas jurídicas. Pero esos datos pueden incluirse con las especificaciones temporarias y se le puede dar a la gente menos información.

Una de las cosas que dijo SSAC es, hagan la información que esté disponible en función de lo que exija la ley, eso es muy importante,

pero no sobreapliquen la ley, brinden acceso en función de lo que establezca la ley. Y esas son dos cosas diferentes.

Con los servicios de representación, hay personas que no están sujetas a GDPR y que podrían igual brindar sus datos.

BRUCE TONKIN: No hablaba de personas físicas, entonces.

GREG AARON: Estamos hablando de privacidad y representación. Hay una superposición en estos dos casos.

Además, quiero decir que SSAC estableció que los registros extensos son una buena idea, por algunas razones de coordinación, de seguridad y estabilidad, y algunos de estos no tienen nada que ver con la provisión de la información.

NICK WENBAN-SMITH: Voy a hablar del tema de servicios de privacidad y representación. Creo que la implicación de esta pregunta es que hay un gran supuesto de que lo que está en la especificación temporaria, que permite que reduzca la cantidad de datos personales, termine siendo una política permanente. Si esto sucede, creo que la pregunta sería, si los datos personales de las personas no van a estar expuestos en WHOIS público, ¿para qué necesitamos esto de la privacidad? Hay sistemas en Europa donde la privacidad se ha incorporado en las operaciones de los registros y algunas personas se benefician de la protección de

datos, como ya dijimos. Sin embargo, siempre hubo demanda por servicios de privacidad y representación. A veces por conveniencia administrativa o por confidencialidad comercial, para proteger algún nombre, etc. entonces, creo que todavía estamos al principio de esto. No lo sabemos, pero estoy seguro de que habrá demanda de estos servicios, pero también pienso que será menor de la que hubo hasta ahora.

BRUCE TONKIN: Gracias.

Hadia.

HADIA ELMINIAWI: Estoy de acuerdo con todo lo que se dijo. Solo quisiera agregar que, si hablamos de la prestación de servicios de privacidad y representación según GDPR, estos proveedores de servicios también tendrán derecho y estarán autorizados a compartir los datos en ciertos casos. Entonces, no estoy segura de que realmente necesitemos servicios de representación en este momento.

BRUCE TONKIN: Chris.

CHRIS LEWIS-EVANS: Con respecto a los servicios de privacidad y representación, con respecto a la pregunta que se hizo antes, dentro de estos servicios no

hay una forma uniforme para pedir datos cuando estaban estos servicios implementados. Habría que pedir información de diferentes formas a los que prestaban estos servicios. .BERLIN no recibió muchos requerimientos. También tenemos que ver qué pasa en el trabajo del grupo anti phishing y una revisión de RDS2. Ya se dijo antes que no hay una forma unificada de solicitar acceso ni de dar acceso, y ese es uno de los problemas que vemos. Realmente en este momento no sabemos todavía. Aparentemente, pasó un tiempo desde que se implementó el GDPR, pero creo que tenemos visto el impacto total que va a tener la especificación temporaria sobre las solicitudes y la cantidad de solicitudes. Las cifras que tenemos hasta ahora son útiles, pero quizá no sean las definitivas.

Y Milton dijo que primero habría que crear una política, y con esta política podríamos definir un modelo de acceso unificado y debemos hacer correctamente esta política para tener un modelo lícito y legal y tener acceso a los datos.

BRUCE TONKIN: ¿Alguien tiene alguna pregunta sobre el tema de la política de privacidad y representación?

CYRUS NAMAZI: Soy Cyrus Namazi. Soy parte de la GDD en ICANN. Simplemente quería aclarar algo con respecto al trabajo de implementación de políticas en GDD y todavía quiero decirles que no dejamos de trabajar en ningún área, ni siquiera en el área de servicios de privacidad y presentación.

Quiero decir esto porque nos hemos dado cuenta de que en este momento no tenemos suficiente información como para crear el marco legal, correcto, para promover el modelo de acreditación, para avanzar con este modelo de modo que se justifique en términos de la eficiencia del trabajo y su posibilidad de aplicación. No tenemos claridad suficiente debido al GDPR y no tenemos claridad con respecto a algunos de los elementos del modelo de acreditación. Entonces, considerando cómo va cambiando la situación y el hecho de que todavía no se ha sentado totalmente el polvo que nos explicaría cómo entender las consecuencias del GDPR, básicamente estamos avanzando con el trabajo de implementación al ritmo al que se va recibiendo la información, que sea útil, para que no desperdiciemos tiempo avanzando con algo que probablemente cambie en el futuro cercano. Y esto no se limita solamente al área de privacidad y representación, vemos algo similar en los casos de la implementación del WHOIS extenso, donde la política ya se definió, ya fue ratificada por la Junta hace bastante tiempo. Y en ese caso, lo que nos impide avanzar rápidamente es que los registros y los registradores deben llegar a un acuerdo en cuanto a cómo van a manejar los acuerdos entre los registros y los registradores. El Acuerdo de Registros/Registradores, el RRA.

Hay otros programas. Tenemos 13 en nuestra organización que tienen que ver con los servicios de datos de registración, todos se van a ver afectados cuando entendamos mejor el GDPR, su impacto y la forma en que el trabajo en políticas y los servicios relacionados con RDS deben ser modificados en el futuro.

BRUCE TONKIN: Creo que usted está señalando un punto importante, Cyrus, algo que ya se dijo antes, el tema de una solución oportuna, porque lo que estamos viendo, y usamos WHOIS extenso como ejemplo, es que esa política se desarrolló hace más de cinco años. No me acuerdo exactamente. Yo no estaba en el Consejo de la GNSO, así que fue hace mucho tiempo. Pero creo que el tema es que el mundo va cambiando, avanza. Las normativas han cambiado significativamente en los últimos años y esto hace que debamos repensar todo. Pero como comunidad y organización deberemos ver cómo podemos responder a los cambios a medida que tienen lugar. Y creo que el desafío en relación al WHOIS extenso ahora es ver si todavía sigue siendo la herramienta adecuada, especialmente considerando los cambios en las leyes de privacidad, especialmente el GDPR. Aparentemente, debemos ahora esforzarnos por hacer correctamente este PDP para establecer correctamente los requerimientos para entender por qué recolectamos datos y establecer estos requerimientos, porque muchas de estas cosas se hicieron en forma paralela. Pero ahora tenemos que ir a lo fundamental, por qué recabamos los datos. Y WHOIS en el pasado tenía por objetivo permitir la competencia, permitir que se transfirieran dominios de un registrador a otro. Entonces, si vamos a describir un objetivo, ese era el objetivo del WHOIS en el año 2000. Y creo que, como comunidad, ahora deberemos escuchar cuál es el nuevo objetivo. Eso es lo principal, establecer correctamente el objetivo o propósito.

Los servicios de privacidad y representación, esto tiene que ver con un debate sobre el acceso. También tiene que ver con el almacenamiento de datos porque las tecnologías que existen hoy permiten almacenar la información de forma distribuida. Como dijo Milton, podemos tener una página de WHOIS o una página de solicitud de información en la página de ICANN. Puede enviar esa solicitud al registrador pertinente, que utilizara su legislación local para responder a esa solicitud.

CYRUS NAMAZI: Gracias, Bruce. Creo que usted señaló otro componente importante en este entorno que va cambiando, porque como ustedes saben, estamos por implementar el RDAP, que es una plataforma totalmente diferente al protocolo de WHOIS que ya es antiguo, está desactualizado. Y esto nos lleva a plantear las preguntas que usted hizo: dónde almacenamos los datos, cómo se tiene acceso a esos datos. Y creo que con RDAP podemos llegar a lo que yo llamo una plataforma del siglo XXI, una plataforma escalable, que puede modificarse y cambiar considerando cómo va cambiando el mundo de la privacidad en todo el mundo y también nos permite desarrollar el tipo de sistema y servicios de datos de registración que realmente puedan avanzar en forma oportuna a medida que cambia el escenario.

BRUCE TONKIN: Gracias. Número uno.

VOLKER GREIMANN: Muchas gracias. Soy Volker Greimann, de Central NIC. Quisiera volver a lo que yo considero puntos de distracción que fueron mencionados antes. La distinción entre personas jurídicas y físicas. Yo creo que esa distinción no es incorrecta. El GDPR no está sobreprotegiendo, porque creo que quizá no se entiende bien qué es lo que protege el GDPR. El GDPR no protege los datos personales, porque protege los personales que quizá se incluyan en los datos brindados por una persona jurídica. Entonces, si se registran los datos de una empresa y la empresa decide informar los datos personales de sus empleados, su correo electrónico, su teléfono, los datos del registratario… esos son datos personales. No podemos hacer esa diferencia. No sabemos si el registro de una persona jurídica incluye los datos de una persona física. Pero esos datos deben ser protegidos de la misma manera.

Entonces, si decimos si una registración se hace por una entidad privada o una persona jurídica, no sirve para determinar si los datos deben ser protegidos o no, según la especificación temporaria. Gracias.

BRUCE TONKIN: Número dos.

DEAN MARKS: Hola, yo soy Dean Marks, de la coalición de responsabilidad online. Quiero volver a algo que dijo la Sra. Monti antes, de que el GDPR incluyen normas que existen desde hace mucho tiempo y hablando del PDP de desarrollo de políticas de privacidad y representación. Este

es un proceso que llevó a una conclusión en 2016 cuando el GDPR ya se estaba debatiendo, ya se conocía, todo lo que tenía que ver con la ley de privacidad, qué es lo que iba a pasar a medida que avanzaba en el proyecto de GDPR.

Entonces, no entiendo por qué ahora se ha pausado hasta que haya más claridad, cuando todos sabemos que el GDPR no responde todas las preguntas, que el GDPR no aporta claridad para todos los detalles. Y, además, como dijo la Sra. Monti, este proceso de múltiples partes interesadas es el lugar para lograr un equilibrio. Habíamos logrado un equilibrio en el PDP de servicios de privacidad y representación. Fue aprobado de forma anónima por el Consejo de la GNSO. Fue aprobado de forma unánime por la Junta Directiva de la ICANN. Es un paso muy importante que nos ayudará a lograr este equilibrio. Y, además, ¿de dónde vamos a obtener esa claridad, Cyrus? Creo que, si avanzamos con los servicios de privacidad y representación, la comunidad de múltiples partes interesadas ayudará a brindar claridad. Yo creo que ICANN Org no está ayudando en nada a la comunidad de múltiples partes interesadas.

BRUCE TONKIN: Cyrus, ¿podría darnos algunos ejemplos más específicos de cuáles son los obstáculos que usted veía para la implementación?

CYRUS NAMAZI: Muchas gracias. En realidad, no quería seguir absorbiendo todo el debate de este panel. Entiendo lo que usted dice, Dean. Y voy a dar

una aclaración. No hemos interrumpido el trabajo de políticas. El trabajo de implementación de políticas es algo que hemos estado haciendo con usted y otros grupos en el IRT. Y no es una pregunta desde mi perspectiva, desde el punto de vista del personal en cuanto a la importancia o relevancia de la política. La comunidad debe decidir esto. En realidad, tiene que ver con desarrollar el marco legal adecuado para implementar esto. Y hemos visto esto trabajando con las organizaciones de custodia de datos y los acuerdos que tenemos y, por el momento, aparentemente creemos que no tenemos suficiente certeza y confianza de que ese marco legal, necesario para implementar, esté en su lugar.

No tiene nada que ver con la importancia de los servicios de privacidad y representación. Creo que los necesitaremos en el mundo post GDPR, pero no es la organización quien debe decidir esto.

BRUCE TONKIN: Número tres.

SÉBASTIEN BACHOLLET: Buenos días, soy Sébastien Bachollet. Voy a hablar en francés, como siempre.

La diferencia entre personas físicas y jurídicas – bueno, eso me sorprende. Por supuesto que hay diferencias. Como persona física, tengo un nombre, una dirección de correo electrónico. Y si alguien me pide autorización, la puedo brindar. Pero una empresa, una persona jurídica, pueden publicar su información sobre sí mismos. Ellos eligen,

nosotros debemos defender a las personas físicas, y las personas físicas deben organizarse a fin de no publicar información sensible. Todos nosotros tenemos información sobre nosotros mismos, así que es normal que una persona física tenga y maneje su propia información.

ORADOR NO IDENTIFICADO: Estoy de acuerdo con Sébastien. Podemos entender el texto de la normativa.

PETER KIMPIAN: Buenos días. Soy Peter Kimpian, del Consejo de Europa. Voy a ser muy breve hoy.

Solo quiero decir que el Comité de Protección de Datos adoptó una guía sobre privacidad que se publicó esta semana. Estamos todavía concentrados en GDPR. Y esperando la opinión de EPDP. Pero el Consejo de Europa tiene a todos los miembros de la Unión Europea más algunos estados miembros, como la Federación Rusa, Turquía, México y algunos países africanos también.

Entonces hay algunas indicaciones y guías acerca de los estándares de privacidad internacionales, especialmente en términos del último tema, datos individuales y también hay definiciones y principios. Muchas gracias.

BRUCE TONKIN: ¿Alguien quiere hacer un comentario con respecto a este punto? ¿No?

¿Hay alguna otra pregunta allí al fondo? ¿No? De acuerdo.

La otra pregunta que yo tenía creo que ya la cubrimos, creo que ya hablamos acerca de cómo garantizamos que la solución cumpla con otras leyes de privacidad. Creo que ese tema ya lo cubrimos.

Después de haber escuchado los comentarios y preguntas del público, creo que verán que hay ejemplos de cómo podemos pasar fácilmente a otras áreas.

Quisiera saber si algún miembro del panel quiere hacer algún comentario acerca de qué es lo que podemos hacer para llegar a una solución oportuna, ¿en qué medida la comunidad puede ayudar al proceso de desarrollo de políticas? ¿Qué podemos hacer nosotros para que sea eficaz?

FLIP PETILLION: Concienciar. Creo que este debate mostró claramente que la gente que tiene datos, que comparte datos, ayuda claramente a avanzar con este debate. Es importante que la gente sea consciente de esto.

Tuvimos una reunión ayer en la que Göran dijo algo muy interesante. Dijo, “Ojalá tuviéramos direcciones tan largas como antes”. Ojalá lo hubiéramos resuelto antes, mucho antes. Pero bueno, esto es cierto, es un hecho. Tenemos que vivir con esto.

Esto me hizo pensar en el futuro. Y me hizo pensar en qué sentido estaba pensando en él, y me preguntaba lo que nos estamos

perdiendo ahora y lo que va a surgir en el futuro cercano en relación con el acceso.

¿Qué significa esto para la ICANN como organización? ¿Significa que va a asumir más responsabilidades en el futuro?

Durante 20 años tuvimos un sistema UDRP muy exitoso, que está ayudando a los titulares de IP, en particular, a los titulares de marcas comerciales. Esa es una solución para una preocupación en particular.

Y me pregunto si habrá otras preocupaciones que también deberíamos cubrir y para las cuales necesitaríamos abordajes similares en el futuro.

Por ejemplo, lo que es una gran preocupación es el perjuicio a los consumidores, a la gente, a los niños.

Es solo un ejemplo, pero es un ejemplo muy importante.

Honestamente, yo hoy preferiría recibir más *spam*, pero sabiendo que podemos pelear contra las violaciones y contra los daños, mientras esperamos el EPDP.

BRUCE TONKIN: Muy bien. ¿Hay algún otro comentario?

Ashley y después Cristina.

ASHLEY HEINEMAN: Hablo en nombre del GAC. Creo que esta conversación acerca de no distraerse, sí, es cierto, hay algunas áreas que podemos evitar que nos distraigan para poder obtener resultados de manera más oportuna.

Pero, habiendo dicho esto y considerando que este panel no se limita al EPDP, creo que desde el punto de vista del GAC, que nosotros apoyamos mucho en la conversación sobre el modelo de acceso universal que tiene lugar en la ICANN.

Estamos muy agradecidos por el hecho de que esta conversación tenga lugar, en gran medida porque nos permite iniciar el proceso de pensar en esto. Nos da el marco para hacerlo. Y además nos da la oportunidad de empezar a identificar y responder preguntas importantes.

Esto no significa que estamos iniciando el desarrollo técnico ni nada de ese tipo. Eso vendrá en su debido momento.

Pero las preguntas como las que usted hizo a la Junta de Protección de Datos Europea, nos ayudan a formalizar un poco más nuestras ideas de aquí en adelante. Entonces, creo que no es sabio caracterizar las conversaciones del modelo de acceso universal como una distracción. Creo que es una forma de iniciar una conversación acerca de otro obstáculo que debemos enfrentar. Gracias.

BRUCE TONKIN: Muy bien. Cristina.

CRISTINA MONTI: Quería subrayar desde mi perspectiva la sugerencia acerca de que en el futuro lo más importante es lograr claridad, un claro acuerdo y transparencia en torno a las diferentes actividades de procesamiento relacionadas con el sistema de WHOIS y sus propósitos respectivos. Esta es la base.

Una vez que tengamos este acuerdo de las diferentes actividades de procesamiento, entonces era mucho más fácil abordar otros aspectos. Y también quisiera sugerir que mantengamos estas actividades de los diferentes procesos por separado. Porque se podría aplicar una base legal diferente. Entonces, tener esta claridad nos va a permitir avanzar en el sentido correcto.

Esa es mi sugerencia.

BRUCE TONKIN: Gracias. Greg.

GREG AARON: Es importante pensar en el futuro dada la situación actual, porque no pensamos con la suficiente anticipación. Entonces mirar hacia adelante es importante.

El grupo del EPDP está trabajando mucho con temas extremadamente difíciles. Y probablemente este sea un buen momento para que la GNSO y la organización en su totalidad piense en lo que va a pasar en 2019. Ese grupo va a avanzar todo lo posible. Pero la especificación temporaria va a finalizar en algún momento y ese grupo está

trabajando mucho. Y veremos cuán parte de ese trabajo se aprueba, pero quizá no se apruebe todo el plan de proyecto.

Entonces, asegurémonos de que el trabajo continúe y que aquellos que hacen el trabajo cuenten con los recursos necesarios para terminarlo.

BRUCE TONKIN: Hadia.

HADIA ELMINIAWI: Como miembro de ALAC, nuestra preocupación principal y nuestro interés principal es lograr que Internet siga siendo un lugar seguro para todos. Entonces, básicamente, detener y evitar el fraude o el uso indebido del DNS, es algo que consideramos muy importante.

Habiendo dicho esto, una vez más quisiera decir que es muy importante mirar ahora a la industria, a los procesos estandarizados de la industria, a los servicios de acreditación.

Porque si terminamos con una política y estas cosas todavía no están implementadas, ¿cuánto tiempo vamos a tener que esperar hasta que tengamos algo implementable y práctico? Gracias.

BRUCE TONKIN: Creo que hay una pregunta del público. Número uno.

RUDY DANIEL: Hola, soy Rudy Daniel, becario de ICANN 63 del Caribe. Tengo una pregunta general: GDPR, ¿obligó a la ICANN y a la comunidad a ordenar sus cosas con respecto a WHOIS, definiendo entonces elementos de datos y el acceso subsiguiente, así como la metodología de acceso con respecto a la legislación aplicable y mirando hacia el futuro, especialmente con respecto a IPv6, que cada vez se adopta más?

BRUCE TONKIN: ¿Alguien quiere responder?

Milton.

Y gracias, Sr. Becario por hacer su pregunta.

MILTON MUELLER: Sí, definitivamente GDPR forzó a la ICANN a ordenar sus cosas. Greg dijo algo acerca de que no nos anticipamos a lo que iba a ocurrir. Hay alguno de nosotros que lo venimos diciendo en la ICANN desde hace 15 años, que WHOIS es ilegal bajo la legislación de protección de datos. No es que no lo supieran, sino que podían seguir sin prestar atención a esas advertencias.

Entonces es más bien una cuestión política que una falla de anticipación. GDPR, sin duda, nos obligó a reordenar todo.

Para resumir, en cuanto al futuro, estoy de acuerdo totalmente con la Sra. Monti, en cuanto a que el trabajo número uno consiste en identificar los propósitos y la recopilación de datos necesarios para

cumplir con esos propósitos. Luego tenemos que definir cuáles son los elementos de esos datos que se van a exhibir públicamente en WHOIS y cuáles son los que se van a ocultar. Luego podemos trabajar sobre el acceso.

No se trata tanto de que los Gorans y los CEOs estén explorando cuestiones legales sobre el modelo de acceso unificado y que esta sea una distracción. Y, además, que sea prematuro. No sabemos en realidad qué hará el modelo y no lo sabremos hasta que no hagamos el primer trabajo.

Entonces, creo que la razón principal para cuestionar el debate sobre el modelo de acceso unificado es que le da esperanzas a mucha gente en cuanto a que, de alguna forma, este modelo de acceso va a recrear el viejo WHOIS una vez que estén acreditados. Y creo que eso es una distracción porque distrae la atención de la gente de centrarse en lo que realmente vamos a hacer con el WHOIS que tenemos ahora en lugar de pensar en cómo voy a obtener acceso y qué estamos haciendo con WHOIS ahora.

RUDY DANIEL: Quisiera saber si el modelo de acceso universal es una solución rápida.

MILTON MUELLER: Podría ser una solución rápida, pero es extremadamente complicado desde el punto de vista legal, técnico y desde el punto de vista de las políticas también.

No, creo que esa es la principal justificación para iniciar este debate. No va a ser una solución rápida. Va a ser complejo.

Para darles el máximo de los créditos, Göran está tratando de avanzar con estas deliberaciones, pero, al mismo tiempo, está impulsando las conversaciones en un sentido que quizá no sea el correcto. Simplemente tenemos que retrasar el tema del acceso hasta que hayamos terminado con la primera parte, lo cual, una vez más, debería ser algo rápido. No nos debería costar demasiado resolver el primer problema.

HADIA ELMINIAWI: En breve, no sabemos si es una solución rápida porque no estamos hablando del acceso ahora y no vamos a hablar del acceso hasta que no hayamos terminado con el trabajo del acceso restringido. Gracias.

BRUCE TONKIN: Bueno, muy bien. Creo que podemos cerrar la sesión acá. Quisiera agradecer a los miembros del panel por una conversación constructiva. Creo que para llegar a un resultado rápido tenemos que entender los temas, las cuestiones y resolverlas. Ese es un paso positivo.

Creo que escuchamos que no vamos a volver al viejo WHOIS. Apoyo ese concepto y también creo que surgió el concepto de que debemos equilibrar la protección de los sujetos de datos y también brindar acceso a los usuarios legítimos. Hay gran apoyo en cuanto a lograr este equilibrio, tanto en el público como en el panel.

Muchas gracias a todos por haber participado en este panel. Esperamos el resultado exitoso del EPDP.

[FIN DE LA TRANSCRIPCIÓN]