

ABU DABI – Discusión del GAC sobre WHOIS/RDS y el GDPR

Martes, 31 de octubre de 2017 – 11:00 a 11:30 GST

ICANN60 | Abu Dabi, Emiratos Árabes Unidos

THOMAS SCHNEIDER: Podemos comenzar entonces con el tema 22. Esta es una sesión en la cual recibiremos información actualizada acerca del whois y los servicios del directorio de registración y el Reglamento General de Protección de Datos, el GDPR. Esto lo venimos tratando desde hace un tiempo, así que sin más le doy la palabra Cathrin.

CATHRIN BAUER-BULST: Muchas gracias, Thomas. Buenos días a todos. Algunos de ustedes ya estuvieron en la sesión del grupo de trabajo sobre Seguridad Pública. Muchas gracias. Vamos a retomar este tema de la continuidad de la disponibilidad del whois y también el tema de la legislación en materia de privacidad, y específicamente el Reglamento General para la protección de datos.

Creo que tratamos de transparentar en la sesión previa de nuestro grupo de trabajo que esta es una cuestión de importancia significativa para el GAC en su conjunto. Sí bien el GDPR es una normativa regional hay otras legislaciones

---

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

regionales que apuntan a proteger la privacidad y a emitir una norma para la protección de datos. No hay algo como una Internet regional, como sabemos. Tampoco hay un whois regional, como sabemos. Y nos gustaría que esto continuará de esta manera hasta la mundial. Entonces creo que el GAC no puede soslayar esto como GAC en su conjunto.

En el día de hoy vamos a hacer lo siguiente. Vamos básicamente a explicarles cuál es la situación actual en algunos minutos. Explicar por qué esto es importante para todos nosotros en el GAC y cuáles pueden ser los próximos pasos a seguir para nosotros en el GAC. Y también vamos a pensar las posibilidades que tenemos en lo que respecta a conversaciones con la Junta Directiva de la ICANN, posibilidades de brindar asesoramiento, posibilidades en los principios de 2017 respecto del juez para los nuevos gTLD, que para nosotros siguen siendo válidos y aplicables, y también ver como nosotros, como GAC, podemos continuar trabajando para lograr una solución. Tenemos que lograr soluciones concretas, pragmáticas y efectiva. Nosotros como GAC tenemos interés en colaborar en pos de esas soluciones.

Todavía se está cargando la presentación en pantalla, pero mientras tanto podemos darles actualizaciones o información reciente. Ok. Veo que está la presentación en pantalla. Entonces pasamos al temario.

Queremos actualizarlos acerca de lo que ha sucedido desde la reunión ICANN 59, luego hablar acerca de la importancia del whois para el interés público y finalmente ver los pasos a seguir. Nosotros hablamos acerca de este tema en Johannesburgo, pero han sucedido muchas cosas. La ICANN ha convocado a un grupo de acción. Laureen y quien les habla fuimos nominadas en nombre del GAC para colaborar. Hubo muchos aportes de distintas partes del mundo, distintos organismos, acerca de cómo se utiliza el whois. Tienen diversos usuarios que recurren a esta herramienta con fines legítimos y también por supuesto que hay uso indebido del whois. Una oportunidad sería ver cómo podemos identificar y podemos limitar esos usos indebidos. También tenemos participantes de la comunidad, de las autoridades de protección de datos en la Unión Europea y en la Comisión Europea. Y como miembro del personal de la Comisión Europea reiteró nuestro firme compromiso de colaborar con la ICANN para tener una solución respecto de este tema dentro del marco del GDPR. Hay muchos análisis jurídicos que se publicaron y también vamos a tener el jueves una sesión intercomunitaria los invito especialmente a participar porque vamos a tratar este tema en mayor profundidad. Vamos a ver ahora los ejemplos que representan la importancia del whois en cuanto a seguridad pública. Ahora nuestra colega de Canadá, Nadine, va a hablar en francés.

NADINE WILSON:

Buenas tardes a todos. Me llamo Nadine Wilson. Vengo de Quebec y provengo de la Policía Montada de Canadá, y pertenezco a la división de cibercriminalidad. Estoy aquí para hablarles un poco de la necesidad de que estas informaciones de whois sean utilizadas. Nosotros lo utilizamos mucho para luchar contra la explotación infantil sexual. Hemos comenzado utilizando estas informaciones para poder identificar a los sospechosos, ya que las informaciones que figuran en el whois no siempre son válidas, pero nos permiten a veces, cuando cometen errores, poder seguirlos por ejemplo a través de una dirección de correo electrónico válida. Eso nos ayuda a seguir una pista y llega a los sospechosos. Todo esto lo logramos gracias a estas informaciones de Whois.

También es importante hablar del centro internacional de coordinación de la explotación infantil en Canadá. En el año 2016/2017 más de 30000 información que nos permitieron llegar a los autores de explotación infantil. Esto fue gracias a las informaciones de whois. Aquí estamos hablando de niños. No quiero por esto denigrar las otras víctimas, pero les quiero llamar la atención sobre la importancia del hecho de que se trata de víctimas que son niños. Por ello la necesidad de estas informaciones de Whois, que nos permiten actuar rápidamente. Muchas gracias por su atención.

CATHRIN BAUER-BULST: Muchas gracias, Nadine. Ahora vamos a compartir un próximo ejemplo. Vamos a escuchar a nuestro colega de Europol.

GREG MOUNIER: Hola. Soy Gregory de Europol. Quiero contextualizar todo esto. Whois es el primer paso en toda la investigación para combatir el delito. El investigador que utiliza el whois lo hace primero para encontrar un punto de contacto para los nombres de dominio. Si encontramos el nombre de dominio y que no registró podemos empezar un proceso legal y podemos obtener mayor información. Los investigadores y los organismos de cumplimiento de la ley tratan de atribuir un delito a una persona, a un delincuente. Entonces whois nos da información que permite continuar con nuestras investigaciones. No necesariamente vamos a ubicar a un sospechoso en whois, pero sí vamos a tener por lo menos un correo electrónico válido para comunicarnos por ejemplo con registradores. Eso es lo que pasa cuando alguien registra el nombre de dominio, tiene que pagar un servicio, etc.

Entonces uno en whois encuentra cómo se va entrecruzando toda esta información y puede detectar a estas personas, con lo cual no es una solución mágica pero realmente es esencial. A modo de ejemplo aquí vemos un resultado de una búsqueda en

---

whois. Uno puede buscar un nombre de dominio, lo ingresan a base de datos de whois y recibe información. Con esta información tenemos pistas, indicios, que podemos verificar con otras fuentes de información. Por ejemplo, quién registro el dominio, cuándo se creó el dominio, cuando se actualizó por última vez, si sigue siendo válido o no. También vemos la dirección de quién registro el dominio, un número de teléfono. A veces el número de teléfono es el único dato vinculado a un dominio que se utiliza de forma indebida. Aquí tenemos información del registratario. Aquí vemos el nombre de la sociedad o de la empresa que está vinculada con ese dominio. Tenemos dirección de correo electrónico, teléfono, dirección postal, etc.

Quiero compartir usted es el caso de un botnet, una red de robots. Pudimos ver quién estaba detrás de la red y quién la controlaba. Entonces básicamente una botnet es una red de computadoras infectadas que están conectadas a un servidor y reciben órdenes y luego distribuyen un software que contamina a computadoras a cambio del pago de un rescate, un ransomware. Entonces lo que hacemos es encontrar un punto de encuentro en el cual se conectan con el servidor que está siendo controlado. Ah y entonces hacemos una búsqueda de whois, encontramos un correo electrónico, luego invertimos esa búsqueda en whois, y vemos todos los nombres de dominio

---

registrados con el mismo correo electrónico. Quienes no son real en cuentas entonces van a tener distintos correos electrónicos, pero en algún punto encontramos un correo electrónico válido. ¿Qué hacemos? Vamos viendo todos los dominios y podemos encontrar un sitio web que no es privado y ahí tenemos más información que nos indica cómo seguir con la búsqueda y podemos identificar al sospechoso. Repito. Esa no es la solución mágica, pero si quedamos sin el whois gran parte de estas investigaciones no van a llegar a buen término. Gracias.

CATHRIN BAUER-BULST: Gracias, Greg. Ahora tenemos un ejemplo de Laureen Kapin, y luego ustedes también podrán hacer comentarios.

LAUREEN KAPIN: Además quiero mencionar la relación con este tema y por qué el whois es importante. Estamos teniendo esta conversación porque el GDPR, como se ha interpretado e implementado dentro del ecosistema de la ICANN, esta implementación realmente impactará a las agencias de cumplimiento de la ley y a su acceso a la base de datos del whois y también a como el público puede acceder a la base de datos del whois. No quiero pasar por alto este punto porque el GDPR tendrá un impacto en cómo esta información se pondrá a disposición.

---

Les voy a dar un último caso de uso. En los Estados Unidos la Comisión de Comercio Federal se focaliza en cuestiones de protección del consumidor y también hay una agencia que se encarga de hacer cumplir las leyes de protección y privacidad. Nosotros utilizamos la información del whois cuando tenemos que investigar cuestiones de infracción a la privacidad. En este caso, si las entidades envían correos electrónicos con phishing se puede, al descargar este correo electrónico o al hacer clic, descargar un malware o spyware que afectan las computadoras. Entonces nosotros en nuestra organización cuando investigamos este tipo de conductas ilícitas vamos al whois para buscar quién se esconde detrás de estos sitios web y tratamos de proteger la privacidad.

No queremos pasar por alto esto porque el GDPR y el GAC tienen los principios del 2007 sobre el whois y busca encontrar un equilibrio entre el cumplimiento de la ley y los intereses de la privacidad. Estos intereses en materia de privacidad no solamente están relacionados con la protección de la información y la información de identificación de las personas, sino también están relacionadas con las agencias de cumplimiento de la ley y de qué manera se utiliza la información privada, por ejemplo, para causar problemas financieros o un daño a nivel financiero. Estos son ejemplos de uso.



Finalmente quisiera enfatizar el público. Ustedes y nosotros y yo estamos o nos manejamos con comunicaciones electrónicas, nos embarcamos en compras electrónicas, en actividades electrónicas, en las cuales merendamos información financiera confidencial. Información que tiene que ver con la salud y que también es confidencial. Por ejemplo, nosotros utilizamos esta información cuando queremos analizar si hay un sitio web que está manejando información que no es legítima. Entonces cuando queremos tener este tipo de contactos recurrimos al whois y mi organización, en el FTC, sabemos que el público utiliza el whois también para poder resolver sus propias disputas o problemas. Y cuando alguien se encuentra involucrado en una conducta que es ilícita, entonces se refieren a la información del whois para poder también presentar sus reclamos. Y además de todas estas cuestiones de seguridad y de intereses comercial legítimas, los investigadores en materia de delitos cibernéticos y las personas que se encargan de la protección de marcas también quieren garantizar que estos usos sean legítimos. Hay otros muchos usos que se pueden dar y que sean importantes para el público. Por lo tanto, hay una amplia gama de razones por las cuales nosotros como el Comité Asesor gubernamental tenemos que considerar estas cuestiones de interés público en relación a las cuestiones del GDPR y de qué manera esto puede afectar al whois.

CATHRIN BAUER-BULST: Muchas gracias por los ejemplos. Quiero enfatizar también que desde la perspectiva de la Comisión las amenazas a la disponibilidad continua de estos datos ya la accesibilidad no se hace tanto en el GDPR en sí porque el GDPR ofrece herramientas y mecanismos para poder brindar servicios con la metodología del whois. Por el momento no hay ningún proceso implementado que pueda garantizar que hay una sola manera o un enfoque coherente para poder abordar este problema y que nos lleve a una solución. Si no podemos brindar un proceso, los registradores y los registros tendrán que llegar a sus propias conclusiones de manera individual, en lugar de nosotros como comunidad hacerlo. El GAC tiene un rol importante, no solamente las partes contratadas dentro de la ICANN, sino que todos tenemos una parte importante porque esto tiene que ver con el interés público. Estas cláusulas necesitan también contar con la custodia del GAC.

Este proceso coherente tiene que tener un foco para el GAC en relación a cómo vamos a avanzar. Hay un problema y ahora tenemos que ver de qué manera podemos abordar esta cuestión en forma efectiva. Para esto hay tres pasos próximos que queremos poner a su consideración. Uno tiene que ver con el asesoramiento del GAC y también podemos brindar nuestro apoyo para poder trabajar en pos de esta solución y hacerlo no

---

solo desde el punto de vista de la Comisión Europea, sino también como GAC. Así que esta es la oportunidad para que ustedes tomen la palabra y compartan sus puntos de vista.

Tenemos el primer orador. Es el representante de Indonesia y luego Estados Unidos.

INDONESIA:

Muchas gracias. Gracias, Cathrin, y al CCWG por la información y por ayudarnos a comprender esto sobre el GDPR. Quisiera disculparme por mi falta de conocimiento acerca de qué significa GDPR. El GDPR fue establecido por una organización sin fines de lucro y fue adoptado por los países de la Unión Europea. Si es adoptado por los países porque lo queremos transformar en una norma europea. Desde mi punto de vista esto es un estándar europeo.

En segundo lugar, ¿existe algún tipo de coordinación entre este estándar y otras organizaciones como por ejemplo la ISO? Pregunto esto porque en diferentes países incluido Indonesia los estándares son realizados por el gobierno, no por entidades sin fines de lucro. Siendo un gobierno con agencias es más sencillo para nosotros participar. Por ejemplo, Indonesia es miembro de las ISO, de la organización encargada de las ISO. Perdón por hacer esta pregunta.

**CATHRIN BAUER-BULST:** No, no es necesario que se disculpe. El GDPR es el Reglamento General para la protección de datos. Es una ley que fue adoptada por los estados miembros de la Unión Europea y el Parlamento y que va a entrar en vigencia en mayo de 2018. Básicamente regula la forma en la cual las organizaciones y las empresas van a administrar los datos personales. No es un estándar, si no legislación que se ha diseñado específicamente para abordar cuestiones de privacidad y protección de datos fundamentales dentro o bajo el ámbito de la Unión Europea.

**ESTADOS UNIDOS:** Muchísimas gracias por esta sesión. Es de muchísima utilidad. Creo que es el mejor momento para recordarnos esto sobre el acceso al whois y a la información del whois porque tiene una gran cantidad de usos y hay varias partes interesadas, particularmente el gobierno. También sirve para proteger al público. También me complace saber que están llevando esta conversación al rol importante del GAC. Es importante que las partes contratadas de la ICANN cumplan con el GDPR, pero me temo que esto estuvo un poco dejado de lado. Tiene un solo foco y tenemos que tener en cuenta cuán importante es mantener el acceso a esta información. No solo el acceso, sino el acceso

oportuno. Tenemos un sistema que requiere órdenes judiciales para casos en particular.

También quisiera mencionar que esto tiene un aspecto territorial a tener en cuenta. En el caso del GDPR se habla de proteger la privacidad de los residentes europeos, pero en realidad el tema que enfrentamos y particularmente dentro del contexto de la ICANN es que habrá una solución global. Finalmente, esto va a permitir por ejemplo un acceso para los registradores de .com, por ejemplo. También esto nos va a poner en conflicto con algunos acuerdos de libre comercio que tenemos con otros países. Nosotros tenemos cláusulas que dicen que tenemos por ejemplo poner a disposición del público la información de registro de los nombres de dominio. Entonces quería llamar la atención sobre este tema y que consideremos de qué manera podemos utilizar esta información. Esto es importante para lo que hacemos y también considera el impacto que esto tendrá en el futuro cercano al momento de acceder a este tipo de información.

LAUREEN KAPIN:

Muchas gracias por mencionar esta amplia gama de temas tan importantes, que no debemos dejar de lado, con respecto al acceso en general, en particular si hablamos del acceso a esta información por parte de otra jurisdicción. Actualmente, cómo

---

agencia de cumplimiento de la ley dentro de los Estados Unidos, si yo voy a utilizar el whois puedo acceder a la información de los registradores o registros y sus identidades de todas partes del mundo. No tengo que tener una orden judicial. No tengo que colaborar con mis colegas en otras jurisdicciones. No es necesario que me digan: No, usted no se encuentra en su jurisdicción. Entonces no podemos darle información.

Este sistema permite el acceso a la información de manera rápida para poder llevar a cabo mis actividades de cumplimiento de la ley. Esto es un beneficio que va más allá de cualquier medida porque, como dije, este es el primer paso. Esto es un momento crucial para las agencias de cumplimiento de la ley y su efectividad. Además, es importante decir que en ciertas situaciones especiales donde hay que ir más en profundidad y dónde las agencias de cumplimiento de la ley tienen que llevar a cabo procedimientos específicos para obtener información, esto resulta un paso básico para la obtención de la información.

CATHRIN BAUER-BULST: Ya hemos escuchado varios ejemplos de casos donde la información del whois es crucial, pero quizás también es interesante hablar del volumen porque nos focalizamos en las investigaciones de ciberdelitos, pero también estamos tratando de evaluar el impacto. Hay una unidad de ciberdelitos y esta

---

unidad realiza por semana unas 50.000 dentro del whois. Sí pudiésemos imaginar un sistema que incluyese también estas órdenes judiciales, creo que no funcionaría del todo.

Tenemos al representante de Pakistán y luego a Irán.

PAKISTÁN:

Muchas gracias por la presentación y por los ejemplos. El ejemplo que usted nos da noto que el punto de contacto del nombre de dominio puede ser importante. También a veces vemos que los datos del whois son un desafío. También sabemos que la ICANN y su grupo de trabajo están trabajando con respecto a la exactitud de estos datos, pero aquí se plantea un desafío. Por supuesto cualquier persona que esté intentando este tipo de desafíos, estas cuestiones, debe contactarse con el punto de contacto del nombre de dominio, pero el Registrador no actualiza esta información. Por lo tanto, esto es un desafío para la comunidad de Internet. Como ustedes saben, hay muchos ccTLD con IDN que han sido lanzados por la ICANN y esto también presenta un desafío para la base de datos del whois porque tenemos también a los nombres de dominio en Unicode, que han sido convertidos a ASCII, lo cual también presenta un desafío.

También el programa de los nuevos gTLD, que fue lanzado con éxito en el 2012, y tenemos la guía para el solicitante en donde se

menciona claramente que el solicitante debe brindar servicios de Whois a sus usuarios. Sin embargo, la ICANN deberá verificar que estos datos del whois estén accesibles. Entonces la accesibilidad a estos datos del whois continúa siendo un desafío. Así que aquí tenemos dos desafíos. Uno tiene que ver con la exactitud de los datos del whois y otro tiene que ver con la accesibilidad. Así que me gustaría saber cuáles son sus recomendaciones o las recomendaciones del grupo de trabajo.

CATHRIN BAUER-BULST: Muchas gracias. Las actitudes algo en lo que el grupo de trabajo se encuentra trabajando, pero en esta sesión me gustaría proponer que nos focalizamos en este punto porque en la semana habrá otra sesión para abordar este tema. Tiene la palabra Irán, luego Ucrania, y luego Países Bajos. Y luego el Reino Unido. Adelante el representante de Irán.

IRÁN: Muchas gracias. Creo que este es un tema que hemos debatido más temprano esta mañana y me parece que es un tema sumamente importante. Todos los gobiernos, todo el mundo está interesado en este tema. Cuando uno recibe un correo electrónico sospechoso o hay un sitio web que es sospechoso a veces se obtienen cientos de correos electrónicos. y esta información muchas veces está disponible para otros. Entonces



¿esta información es la que ustedes comparten con otras personas? Básicamente me refiero a interpol para saber si comparten su información rápidamente y si tienen interconexión con otras oficinas de Interpol en otras partes del mundo, si están al tanto de esta situación.

Y mi segunda pregunta pues sí por alguna razón, no quiero entrar en detalles, pero ¿hay alguna restricción de algún país para tener acceso a esta información? Porque a veces hay decretos, instrucciones que no permiten que estos servicios están disponibles para un país particular por diferentes razones. Es un tema muy importante. No tener ninguna restricción es muy importante porque esa información es sumamente importante, de naturaleza muy importante, y afecta otras decisiones, etc. Así que me gustaría saber si hay un acceso completo de todos los países a todos los tipos de información. Quizás esto pueda no estar disponible para todos los países y quizás no se aplica en este caso.

GREG MOUNIER:

Gracias por su pregunta. Si la estructura de back-end está disponible y esto difiere en varios países en el sudeste asiático, sí nosotros tenemos que tomar esta infraestructura y tenemos que contactarnos con la Policía Local, sí, lo hacemos a través de Interpol y a través de la corporación internacional de policía y

tenemos las autoridades competentes para que actúen y que avancen con las investigaciones. Si se pregunta se refiere al acceso restringido al whois, por ejemplo, yo sé que la policía de Irán está utilizando el whois, también hay investigaciones que se llevan a cabo en China, en Irán, y que están utilizando esta información, no hay ninguna restricción en cuanto al procedimiento para utilizar este tipo de información.

CATHRIN BAUER-BULST: Tiene la palabra Países Bajos, Reino Unido. Ucrania. Tiene la palabra el representante del país de Ucrania.

UCRANIA: Tengo una pregunta en relación a la legislación, al desarrollo de la legislación. Creo que son aclaraciones importantes. En la Unión Europea, ¿de qué manera ustedes califican a los datos encriptados? Es decir, a lo que se almacena dentro de la Unión Europea. Esta información personal que fue encriptada. No aparece o aparece como información personal para las agencias de cumplimiento de la ley y los administradores o simplemente aparece como información técnica.

CATHRIN BAUER-BULST: Gracias por la pregunta. Yo creo que podemos abordarla después de la sesión. Hasta ahora el whois se encuentra

---

plenamente disponible. Vamos a darle la palabra ahora el representante de Países Bajos.

PAÍSES BAJOS:

Gracias, Cathrin. Creo que el GDPR a veces se subestima. Algo puede suceder dentro de este contexto, pero creo que tenemos que tener en claro algunas cuestiones. Ya no es algo que sea por ejemplo solo de la Comisión o que se aborde solo dentro de la Comisión, sino que los 37 países tienen que analizar cuál sería una posible solución de acuerdo con el GDPR porque estamos hablando de algo que es real, algo que va a ser ilegal en algunos países si no se cumple. Por ejemplo, se han enviado una carta sobre el punto FRL. Hay recomendación edificas y posiblemente esto también estoy de acuerdo al GDPR. Son regulaciones armonizadas así que tenemos que abordar el hecho de que el GDPR estará vigente.

En segundo lugar, por supuesto nosotros reconocemos qué se necesita acceso a los datos del whois, pero hay una forma simple decir: Bueno, sí, se cancelará el nombre o se accederá a través de órdenes judiciales, pero no creo que este sea el caso. Creo que todo tipo de acceso a cierto tipo de datos es posible. Incluso en los Países Bajos, en el registro de .nl, esto se puede utilizar. No es blanco o negro. Creo que limitar el problema sería un tanto simplista.

CATHRIN BAUER-BULST: Muchas gracias. Hizo dos planteos válidos. En primer lugar, todos nosotros estamos juntos en esto, no solo en la Comisión Europea, ni siquiera en sus 27 estados miembros, sino el GAC en su conjunto, qué debe analizar esta cuestión y ver cómo podemos cumplir con esta norma. Claramente hace falta introducir cambios a tal efecto y deberíamos ser un participante clave en la generación de este cambio y en aportar una solución viable. Pido disculpas si dimos una perspectiva un tanto simplista, dado que este es un tema bastante complejo. Lo que tratamos puede transmitir una idea que fuera viable y de darles información actualizada a la brevedad y quizás simplificamos algunas cosas en exceso. De hecho, hay soluciones que están en una suerte de término medio y en algunas partes de la comunidad parece que todo es bastante negativo, pero necesitamos por ejemplo lo siguiente. Si un organismo de cumplimiento de la ley necesita una solicitud para poder llevar acabo sus 50000 búsquedas a la semana eso realmente es un problema.

Ahora le doy la palabra a Reino Unido y luego Palestina.

REINO UNIDO: Soy [incomprensible] del Reino Unido. Gracias, Cathrin. Coincido en gran parte con los comentarios anteriores. No soy experto en

cuestiones jurídicas y no he seguido de cerca las participaciones de los expertos del Reino Unido respecto del GDPR. Lo único que veo es que hay un póster, una ficha en mi oficina en Londres que dice: Prepárense porque está llegando el GDPR. Bueno, en realidad mi pregunta apunta a los casos que acabamos de ver. Hoy por la mañana vimos que existe un propósito en legítimo respecto de estas solicitudes de los organismos de cumplimiento de la ley y los organismos de defensa del consumidor, con lo cual ¿es efectivamente definitivo el hecho de que el acceso con esos fines legítimos en pos del interés público y de la protección del consumidor para poder restregar delincuentes? ¿Es definitivo el hecho de que esto quede fuera de vigencia debido a la aplicación del GDPR a una base de datos del WHOIS?

Esto quizás guarda relación con intervención previa de mi colega de Países Bajos. El impacto del GDPR en realidad no sea tan maravilloso porque si uno tiene un mecanismo o lo que fuere similar a lo que tiene cada uno de los registros de nombres de dominio con código de país, quizás entonces podemos solucionar este problema. Hoy por la mañana estuve en la última parte del grupo de trabajo sobre Seguridad Pública y si hablo de un tipo de acceso por niveles, regulando el acceso, de manera tal de facilitar este tipo de acceso público que necesitamos mantener para evitar que los registros retiren de la lista este tipo de información de contacto, etc. Que lo quiten de la base de

datos del WHOIS, lo cual es una amenaza la integridad general de la base de datos del WHOIS. Entonces quizás las soluciones estén al alcance de la mano y solamente haga falta trabajar con celeridad para tener estas soluciones listas antes de mayo consultando las autoridades de protección de datos de Defensa del Consumidor del orden público. Probablemente tengamos un camino por delante en esta comunidad para lograr.

Entonces mi pregunta es: ¿usted cree que realmente perspectivas de poder solucionar esta cuestión a tiempo, teniendo en cuenta los objetivos legítimos que estuvimos analizando? Entiendo que de algún modo están considerados en el GDPR.

LAUREEN KAPIN:

Usted hace un planteo muy válido. Si no creyéramos en una solución posible no estaríamos aquí. El GDPR tienes estás vías pensadas para lograr un equilibrio entre la protección de la privacidad y los datos que pueden identificar a una persona con el acceso legítimo a esa información. Hay algunas vías específicas contempladas en el GDPR para lograr justamente un equilibrio adecuado entre estos intereses. Si nosotros eligiéramos aceptar el GDPR nuestra misión sería focalizar nos en el interés público, de manera tal que haya un equilibrio adecuado para proteger la información de conformidad con el

---

GDPR, y al mismo tiempo proteger estos intereses y que sean tenidos en cuenta. Es un equilibrio a lograr. Tenemos vías posibles para lograrlo y debemos cerciorarnos de que la ICANN se concentre no solo en los intereses comerciales importantes que están en juego y en evitar la responsabilidad legal, sino también en que haya vías posibles en el GDPR para proteger este interés público también.

CATHRIN BAUER-BULST: Gracias, Laureen. Ahora toma la palabra Palestina.

PALESTINA: Gracias. Anteriormente estuve en un grupo en el cual se trataban los conflictos. Trabajé anteriormente en grupos que hablaban acerca de los conflictos entre las legislaciones y su aplicación en Europa. Y también acerca de las acciones posibles para combatir al delito cibernético y a todas las instancias de uso indebido. Se realizaron muchas sesiones con los RIR y también con los organismos de cumplimiento de la ley. Los RIR deben cumplir las leyes de los países en los cuales están ubicados y probablemente se comete un delito en un país y en otro país ese acto no es un delito. Entonces hay una ley estricta que probablemente pueda abordar ese delito, con lo cual ¿cómo podemos acceder a los datos pertinentes? Anteriormente sufríamos el hecho de que los registradores y los registros no

---

documentaban los datos con exactitud. Entonces cuando queríamos obtener información había cierta dificultad y no había suficiente información ni precisión. Las demás partes deberían trabajar para lograr obtener esta información precisa.

CATHRIN BAUER-BULST: Muchas gracias al representante de Palestina por plantear estas cuestiones, por volver a traer a colación el tema de la exactitud de los datos que tenemos que tratar. De hecho, es un requisito del GDPR.

También usted pregunta acerca de las soluciones y del acceso a los datos. Con esto pasamos a ver los pasos a seguir. Nosotros respecto de las posibles vías para el GAC sugerir y amos plantear este tema y la importancia de la participación del GAC. Plantearlo ante la Junta Directiva, también ver cómo redactar esto en el asesoramiento del GAC, y ver maneras de proponer soluciones prácticas. Después de la sesión intercomunitaria el jueves, vamos a tener una segunda sesión para hablar acerca del whois y del GDPR y podemos retomar este tema.

En pantalla estamos viendo algunos puntos que resumen las perspectivas previas del GAC, sobre todo teniendo en cuenta los principios sobre whois del año 2007. Para nosotros continúan siendo una muy buena fuente de información y orientación, qué tiene que ver también con la política sobre whois. Entonces



deberíamos reiterar que estos principios deben seguir siendo aplicables y se los debe respetar. También que el whois debe seguir siendo de acceso público para poder luchar contra uso indebido, contra fraude y para poder tener transacciones y comunicaciones en línea de manera diligente. Asimismo, poder ayudar a quienes trabajan en protección del consumidor y en investigaciones y organismos de cumplimiento de la ley y prevención del delito. También poder alentar a la ICANN a que ejerza la transparencia en sus actividades relativas al GDPR y que dé una oportunidad al GAC de presentar sus comentarios de manera significativa y oportuna y también alentar a la ICANN a que se interrelacione con la Comisión Europea para facilitar debates acerca del proceso de cumplimiento del GDPR. La Comisión Europea no es el único actor en este proceso. Lo que podemos hacer es trabajar con la secretaria del grupo de trabajo sobre el artículo 29. Eso significa que todas las autoridades de la Unión Europea se reúnen y pueden dialogar sobre este tema. Lo que nosotros podemos hacer desde el rol de la secretaria es ayudar a facilitar esas conversaciones, de manera tal que todas las partes estén involucradas y que no se perciba que la Comisión Europea es el único actor en todo este proceso. Podemos entonces trabajar junto con la comunidad de con las distintas autoridades nacionales dedicadas a la protección de datos.

---

Ahora entonces vamos a tener una sesión para preparar la reunión del GAC con la Junta Directiva. Podemos seguir hablando acerca de estos pasos a seguir. Gracias por su participación.

THOMAS SCHNEIDER: Gracias, Cathrin. Con esto finalizamos la sesión número 22. En 30 segundos vamos a pasar a la sesión número 23. Muchas gracias por su participación. Seguramente vamos a tener en pantalla el temario propuesto para nuestra reunión con la Junta Directiva.

**[FIN DE LA TRANSCRIPCIÓN]**