

---

COPENHAGUE – Reunión del GAC: Comisarios para la protección de datos del Consejo de Europa  
Lunes, 13 de marzo de 2017 – 17:00 a 18:30 CET  
ICANN58 | Copenhague, Dinamarca

THOMAS SCHNEIDER: Por favor, les pido a todos que tomen asiento. Bienvenidos a esta sesión especial del GAC por iniciativa nuevamente del Consejo de Europa. Le quiero agradecer a todo el equipo, que incluye a expertos en la cuestión de protección de datos. También tenemos algunos colegas de los organismos encargados de cumplimiento de la ley. Aquí estamos en esta sesión con la GNSO en esta sala grande. Me voy a detener porque queremos tener una sesión interactiva con los expertos sobre protección de datos y cumplimiento de la ley. Johannes, adelante, por favor.

JOHANNES KLEIJSSSEN: Gracias, Thomas. Voy a ser breve para dedicar el mayor tiempo posible a la presentación de los miembros del panel. Quiero agradecer al GAC por permitirnos mantener este intercambio de ideas sobre protección de datos con los expertos en la materia. Tuvimos una discusión entre las comunidades sobre este tema muy interesante y por los comentarios quedó claro que hay muchas cuestiones que indican que esta no debería ser una única discusión sino el punto de inicio de todo un proceso.

---

***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.***

---

En la sesión anterior, yo presenté al Consejo de Europa. Ustedes saben que nosotros somos observadores del GAC desde el año 2010 y que hemos presentado tres informes. El más reciente es sobre las solicitudes para TLD en cuanto a las implicancias desde el punto de vista de derechos humanos. Les quiero decir que para el evento de hoy, el debate que se está desarrollando es sumamente oportuno y a la vez necesario. Cada vez más existe un riesgo y una realidad con respecto a obligaciones conflictivas por un lado y también obligaciones desde el punto de vista de los contratos y la protección de datos que son obligaciones vinculantes por el otro lado. Es necesario llevar adelante esta discusión que es oportuna y necesaria, como les decía.

En el Consejo de Europa tenemos el Convenio 108. Tenemos 50 partes y 10 observadores en ese convenio sobre protección de datos. Esto significa que la mitad de los estados en el mundo tienen legislación específica del tema de la protección de datos. Yo soy director de la Sociedad de la Información. El organismo encargado de la lucha contra el delito. Esto les indica que tenemos una comunidad muy fuerte y que trabaja arduamente en este tema. Tenemos una convención de derechos humanos y también tenemos unos 60 convenios sobre el derecho penal, algunos ratificados por 60 estados en todo el mundo. Nuestro convenio sobre el ciberdelito tiene 50 signatarios y también

---

cooperamos en el desarrollo de capacidades con 125 países. Hay mucho que se hace en las fronteras de Europa.

Si me permiten, quiero decir algo que ya se dijo anteriormente. Esta es una fuerza para el bien. Esto implica que hacemos frente a enormes riesgos. Todos en el mundo estamos preocupados con respecto a lo que ocurre con nuestros datos. Hay muchas expresiones de esa preocupación. Por ejemplo, la divulgación de información por parte de WikiLeaks, que realmente atrajo la atención de todo el mundo. Esta es otra de las fuentes de preocupación. Dentro del GAC y dentro de la ICANN es necesario tener este debate con la sociedad civil, con las empresas y con los organismos de aplicación de la ley pero también con la comunidad encargada de la protección de datos. Gracias.

ALESSANDRA PIERUCCI: Hola todos. Soy Alessandra Pierucci. En primer lugar, quiero darles las gracias por darme la oportunidad de participar en este evento sorprendente. Realmente estoy sumamente agradecida y honrada de estar aquí. Estoy aquí en calidad de presidenta del comité consultivo para el Convenio 108 que es un convenio del Consejo de Europa para la protección de datos personales. Este comité consultivo está compuesto por muchos representantes de quienes son signatarios de este convenio pero también observadores. Que participan activamente de las discusiones en

---

nuestro comité. Nuestro comité es responsable esencialmente de interpretar las cláusulas principales del Convenio 108. También es responsable de la implementación de los principios vinculados a la protección de datos en diferentes sectores de interés. Para darles un ejemplo, el comité consultivo aprobó una serie de directrices y recomendaciones que por supuesto luego tienen que ser adoptadas a nivel del comité de ministros sobre protección de datos en varios lugares, como la policía, los sectores públicos, el empleo, los datos de salud, antecedentes.

Quisiera que presten atención al Convenio 108, en particular a dos características principales de este convenio. La primera es que estamos hablando del único instrumento vinculante en este momento, y el primero con respecto a la protección de datos a nivel internacional. Debería decir que el segundo elemento que caracteriza a este convenio es su carácter abierto. Está abierto también a terceros países. Lo menciono porque el Convenio 108 no solamente ha sido ratificado por los 47 estados miembros, como mencionó antes Johannes Kleijssen, los 47 miembros del Consejo de Europa, sino que también acepta la adhesión de terceros. Ese es el caso, por ejemplo, que veremos en la próxima diapositiva de Uruguay, Senegal, que ratificaron el convenio como terceros, y Mauricio.

Hay otros países que actualmente están en el proceso de ratificar el Convenio 108. Ustedes ven los nombres aquí en la

---

pantalla: Marruecos, Túnez, Cabo Verde y Burkina Faso. También debo decir que tenemos una participación igualmente activa de los observadores. Más que nada, organizaciones internacionales pero también otros países como Estados Unidos, Canadá, Australia, Corea del Sur, México e Indonesia. De hecho, tenemos la solicitud para acceder como observadores de Japón y Filipinas. Esto hace un total de más de 60 países que contribuyen al trabajo que realizamos en nuestro comité. Siguiendo, por favor.

Incluso sin la diapositiva, continuamos dándoles algunos indicios de este convenio. El Convenio 108, como se firmó a nivel de la Unión Europea, fue sometido a un proceso de modernización. Ustedes entenderán que los principios vinculados a la protección de datos contenidos en el Convenio 108 tenían que ser actualizados por el impacto de las nuevas tecnologías y la globalización. Este tipo de proceso de modernización comenzó con la participación de muchas partes interesadas. De hecho, la apertura de ese proceso se dio a través de unas consultas con contribuciones realizadas por muchas partes interesadas, incluidos los sectores privados.

El Comité de Ministros del Consejo de Europa es quien tiene la responsabilidad de concluir los detalles del proceso de modernización de este instrumento. Voy a hacer unos breves comentarios con respecto a lo que todavía es válido a partir de la

---

estructura general del Convenio 108 y cuáles son los elementos nuevos de este convenio modernizado. Me atrevería a decir que la estructura general que dio lugar a este convenio tiene que ver con un lenguaje universal. Este sigue siendo un elemento válido del convenio antiguo. Se hace referencia a principios generales y no detallados porque tiene que hablar con una cantidad importante de países. También tiene un lenguaje tecnológico neutral para evitar que se vuelva obsoleto demasiado pronto y garantiza una congruencia con el marco de la Unión Europea. Es importante tener esto en cuenta. Por supuesto, hay un vínculo entre el Convenio 108 y la Unión Europea con su marco de protección de datos, como fue enfatizado por la nueva reglamentación que especifica la posibilidad de ingreso de un tercer país al Convenio 108 como un elemento que puede ser considerado de importancia para la evaluación de la adecuación de ese tercer país.

Otros elementos que se han fortalecido en la estructura general del Convenio 108 están aquí representados en la pantalla. Su principio de proporcionalidad y de minimización de los datos. Se trata de un principio vital para la protección de datos. El principio de responsabilidad en el sentido de rendición de cuentas. Es decir, que los controladores y procesadores de datos tienen que asegurarse de cumplir con los principios de protección de datos por escrito en la documentación pero

---

también en la práctica. Transparencia, que ha sido también ampliada. Aquí significa que el titular de los datos debe estar en conocimiento de que se están procesando los datos personales vinculados a él. También tiene que saber cuál es el ejercicio de sus derechos. Por ejemplo, en el convenio se ha introducido el derecho a no ser sometido a una decisión automatizada sin tener posibilidad de expresar la opinión personal.

La seguridad de los datos es otro elemento que ha sido fortalecido en el nuevo convenio. Hay disposiciones específicas sobre la transferencia de datos a nivel internacional y de las autoridades de supervisión que han sido incluidas. Estos temas, por el momento, son parte del protocolo adicional para el Convenio 108. Siguiente diapositiva, por favor.

Lo que acabo de hacer es una reseña muy general de los principios centrales del Convenio 108 pero el mensaje que quiero transmitirles es la voluntad del comité consultivo del Convenio 108 de entablar un diálogo con la ICANN y actuar como posibles interlocutores en caso de que haya preocupación y problemas por cuestiones de privacidad. Yo ya he hecho hincapié en el hecho de que el comité consultivo está acostumbrado a trabajar en un ambiente multilateral, de múltiples partes interesadas, con mucha apertura a todos los países del mundo. Estamos ansiosos por contribuir a este trabajo. Muchas gracias.

---

THOMAS SCHNEIDER: Ahora Joseph Cannataci, el relator especial de Naciones Unidas sobre el derecho a la privacidad.

JOSEPH CANNATACI: Gracias, Thomas. Creo que los que estuvieron en la sesión anterior comprenderán por qué es tan fácil para mí hablar después de la presentación que hizo Alessandra. Hay dos organizaciones, la organización madre que es el Consejo de Europa y la Unión Europea, que se creó después. Les quiero dar algunos datos históricos para que tengan presentes. El convenio del que estuvo hablando Alessandra existe desde 1981 y necesitaba algo de modernización. Fue ese convenio el que inspiró la creación de la Unión Europea porque no era una unión en ese momento. En junio del 81 recurrió a 7 de los 12 miembros y les dijo: “El Consejo de Europa es algo bueno. ¿Por qué no se suman a él?” Y no había suficientes miembros que decidieran adherirse a este Consejo pero entre ese momento, del año 90 al 95, hubo una directiva que fue emitida, que ahora ha sido modernizada y se ha transformado en la reglamentación sobre protección de datos que se llama GDPR.

Creo que este es un contexto importante a tener en cuenta porque si pensamos en los países fuera de Europa, desde una perspectiva global y mundial, hubo un ímpetu que se extendió a



---

partir del GDPR, esta reglamentación sobre protección de datos general. Cómo las compañías de determinados países fuera de Europa tenían que tener en cuenta esta reglamentación. Esto hacía que muchos países quisieran pasar a un régimen más estructurado desde el punto de vista de la privacidad. Estos iban a tender a acercarse a ese marco que fue propuesto por el Consejo de Europa como lo describió Alessandra.

Creo que esa es la primera parte. Debe recordarnos también otras iniciativas que han sido adoptadas para el transporte de datos y la policía. Si hablamos de cooperación, creo que primero podemos hablar del ámbito que atañe a las corporaciones y luego pasar a la esfera más pública. La transferencia de datos se da por dos motivos, porque los organismos de protección de cumplimiento de la ley, la policía y los servicios de inteligencia lo requieren. Hablemos un poco de esto. No sé si Caroline va a hablar luego de esto, sobre el marco que ya está en existencia con la INTERPOL pero primero debemos hablar de la Convención sobre el Cibercrimen. Hay otros 44-50 países. Por lo menos 47, ya acercándonos a 50 que se han adherido a esta convención, la 185, sobre el cibercrimen.

La sección de 32 de esta convención tiene la intención de facilitar la transferencia de datos entre una autoridad y la otra. Ha habido discusiones durante mucho tiempo con respecto a cómo lograr eso. Si ustedes sienten que hay un pero que viene a

---

continuación, así es. Esa convención, con todas sus imperfecciones y todas sus falencias, solamente está diseñada para lograr una cosa y es la transferencia de datos para los organismos de cumplimiento efectivo. Si se fijan en la sección 14 de ese convenio sobre la ciberdelincuencia, en realidad no está diseñado para encargarse de la parte que tiene que ver con inteligencia, para el intercambio de datos fuera del ámbito de la policía. Es importante recordarlo porque muchos de ustedes van a entablar un diálogo con los clientes y los clientes les van a decir: “No, Snowden dijo esto y esto es lo que pasó”. Esto es lo que tiene que ver con la privacidad.

Este convenio sobre ciberdelincuencia no estaba diseñado para eso. Habrán visto el informe que yo presenté al Consejo de Derechos Humanos en las Naciones Unidas la semana pasada. Yo hablé acerca de esfuerzos que se están llevando adelante fuera del marco de las Naciones Unidas en este momento pero que posiblemente se incorporen a él en el próximo año, que van a llevar a la preparación de otro acuerdo. Tal vez con otro tipo de abordaje como en rodajas para el derecho sobre ciberseguridad, lo que se transformará en un instrumento legal en el ciberespacio. Básicamente tenemos aquí una intención de hacer frente a la ciberdelincuencia con el convenio sobre ciberdelincuencia. También la intención de atacar todas las cuestiones vinculadas con los datos personales que tienen las

---

corporaciones y los gobiernos en el contexto de los países que han adherido al Convenio 108, ¿pero qué pasa con el resto de las leyes en este sentido?

Esto no va a ser fácil de solucionar pero hay muchos otros ejemplos de cosas difíciles que ha solucionado el mundo y eso es excelente. Esto tiene que ver con la supervisión y la vigilancia en el espacio cibernético. Tenemos un particular interés entre las comunidades de la ICANN en saber qué pasa con los datos, especialmente cuando los maneja el gobierno, los servicios de inteligencia, pero también qué pasa con las empresas. Tengo un centro de datos en Alemania y hay un tribunal en Nueva York que quiere que yo le brinde los datos que tengo guardados en la India, en Honolulu o en Irlanda. Como gobierno, como ISP o como controlador de centro de datos, ¿cómo se maneja esto? Lo que es peor, ¿cuáles son las medidas de protección técnicas, las salvaguardas técnicas que tendríamos que implementar para facilitar este tipo de intercambio o para asegurarnos de que no haya un uso indebido?

Debo recordarles un par de cosas. No solamente tenemos que mirar el manejo de la identidad desde una perspectiva diferente sino que también tenemos que ver todos los aspectos, muchos otros factores, muchas salvaguardas, medidas de protección que se pueden utilizar para asegurarnos de generar una atmósfera que preserve la privacidad de los datos en el espacio cibernético

---

donde podamos tener una mayor confianza, sobre todo desde el punto de vista de los ciudadanos. La semana pasada, como lo dijimos también, esto va a ser bueno para la privacidad, para los ISP, para los ciudadanos, para los gobiernos y para las empresas. Gracias.

THOMAS SCHNEIDER: La próxima es la señora Caroline Goemans-Dorny, la oficial de protección de datos de la INTERPOL.

CAROLINE GOEMANS-DORNY: Muchas gracias por haberme invitado. La semana pasada de hecho fue la conferencia anual de la INTERPOL, de la reunión de las oficinas centrales nacionales. Es una conferencia anual que sirve como brainstorming. Es una oportunidad de hacer discusiones más sencillamente que en la asamblea general, donde los temas son más candentes. Fue una sesión de brainstorming la semana pasada. Se invitó a unos 190 países. Como saben, la INTERPOL es una organización global de sociedades y corporaciones y policía con 190 países miembros. Una de sus tareas es actuar como un centro de información de bases de datos policiales mundiales.

Uno de los paneles trató de la solidez de las normas de protección de datos. Fue un panel multidisciplinario y me

---

pidieron participar y presentar mi opinión sobre cuál era el valor agregado que tenían estas normas de protección de datos desde el punto de vista de la INTERPOL. No voy a dar ninguna novedad. En cambio, voy a hablar de lo fundamental. Para hacer una acción policial efectiva hay que tener confianza. Aquí es donde el marco de protección de datos puede ser de ayuda. No solo a los fines de crear ese ecosistema de confianza en el cual la cooperación policial puede darse concretamente sino que también es una cuestión de reputación. Como ustedes saben, la constitución de la INTERPOL se refiere específicamente a la declaración universal de derechos humanos que incluye no solo el derecho a la privacidad sino otros derechos tales como el de libertad de expresión. Así, la INTERPOL actúa como una cámara compensadora en la revisión de la calidad jurídica y lícita de la información.

Desde 1982, las reglamentaciones sobre la protección de datos existen. La inversión en el largo plazo y la creencia en el valor agregado en el largo plazo de la protección de datos es algo que ha sido asumido desde hace mucho tiempo. Es como construir un cimiento sólido para un edificio. Las normas de la INTERPOL se basan, de hecho, en el principio del Convenio 108, que es de diseminación universal. A lo largo de los años, las normas sobre protección de datos fueron elaboradas, ajustadas y adaptadas a los diferentes casos. En el año 2011 terminamos elaborando un

---

código que, en nuestra opinión, es una guía muy buena para los policías, muy detallada, donde encontramos una respuesta a todas nuestras preguntas.

La protección de datos es de hecho un proceso dinámico. Este es otro punto que la INTERPOL siempre ha dado por supuesto. Son reglas que deben actualizarse de manera continua. El primer conjunto de reglas, como dije, datan de 1982. Desde la última actualización de 2011, hemos añadido algunas más. Estos son los aspectos fundamentales. Hace un par de días conté que había un par de reglas nuevas. Hacemos una actualización cada tres años. En lo que hace a los desafíos, tenemos una nueva versión sobre temas específicos tales como la cooperación entre los organismos de aplicación de la ley con el sector privado. Aquí ha habido una gran evolución. Nuestros organismos en el año 2004 no querían saber nada de la cooperación con el sector privado. Esto ha cambiado mucho y ahora es necesario contar con un marco.

La manera en que nosotros abordamos los temas nuevos es que no necesariamente tenemos nuevas reglas de inmediato sino que preferimos establecer proyectos que tienen un buen marco, evaluar esos proyectos durante un año y después considerar si esta experiencia puede servir como material de reflexión para elaborar nuestras propias reglas. Ahí es donde nosotros las elaboramos. Así venimos trabajando desde entonces. Esperamos

---

que en un par de años o antes tengamos reglas para el trabajo con el sector privado.

Como decía entonces, la INTERPOL actúa como una cámara compensadora. Se revisa la calidad, su legitimidad, su licitud. INTERPOL publica avisos o notificaciones que indican si existe el propósito de arrestar a una persona. Se hace una revisión de manera cerrada o confidencial antes de divulgar esta información al público. Se hace de manera restringida en el sitio, con criterios específicos y umbrales. Además de estas reglas dinámicas, está esta ventaja de que las normas o las reglas son dinámicas. Todos están cubiertos por estas reglas. Generan cierta interoperabilidad entre los 190 países. Se basan en distintos pilares. Está bien tener reglas pero es necesario implementarlas de manera eficaz. Hay una supervisión efectiva. Tenemos capacitaciones regulares pero lo importante en todo este proceso es tener un sistema, no solo elaborar reglas sino también procesos y desarrollar la tecnología. Tenemos la regla de los 190 oficiales específicamente dedicados a la protección de los datos para cada oficina central.

Yo tengo el privilegio de coordinar su trabajo. Es un trabajo constante. Es un placer para mí dirigir esta tarea. Creo que potencia estos umbrales globales que tiene la protección de los datos de manera internacional. Como decía, tenemos que ver la implementación de los principios de protección de datos y de

---

privacidad como un área multidisciplinaria. No trabajar solo con lo legal o interesarnos solo por lo legal sino que también los procesos comerciales son interesantes y la elección de las tecnologías correctas. Como dije en la reunión anterior, estamos hablando aquí de principios de buena gobernanza. La exactitud de lo que se procesa, qué es lo que se procesa, por qué se procesan estos datos. El cumplimiento también es otro de los principios de buena gobernanza. Cuando se tiene buena gobernanza, se tienen buenos negocios. Es decir, la protección de datos en la INTERPOL es un trabajo que se ha dado de manera constante desde hace años y es visto como la base para elaborar la confianza y la reputación de la organización. Muchas gracias.

THOMAS SCHNEIDER: El siguiente es el supervisor europeo para la protección de datos, Giovanni Buttarelli.

GIOVANNI BUTTARELLI: Muchas gracias por la invitación a participar en este panel. No voy a repetir lo que he dicho en el panel anterior pero una pregunta que seguramente han escuchado de todos nosotros es por qué nosotros, los europeos, estamos dictando reglas para el resto del mundo. Es una pregunta legítima. Pero creo que si analizamos los detalles y elementos relevantes llegamos a la sencilla conclusión de que todos estos ejemplos y leyes aisladas



---

del Consejo de Europa, la OECD, los países de Asia, de APAC, muestran que existe una interoperabilidad en la noción moderna de lo que es la protección de datos. Es algo interesante que afecta a 120 países en el mundo. El profesor Greenleaf analizó la filosofía de estas legislaciones nacionales individuales. El resultado del análisis es que fuera de la Unión Europea, fuera del marco del Consejo de Europa, más de la mitad de estos 120 de los que estamos hablando, por ejemplo en América del Sur y en África, ya siguen un modelo que se asemeja al europeo.

Parece ser que existe una preocupación creciente por la necesidad de tener una respuesta común a problemas similares. Yo observo una tendencia. Cuando queremos apartarnos de los requisitos legales, deberemos alejarnos de las formalidades que no tienen sentido y acercarnos a las medidas de protección efectivas. Ese es el objetivo de la protección de datos. Con principios y valores que hagan que las sociedades en la práctica sean más fáciles de administrar. El verdadero desafío, por ejemplo en el GDPR de la Unión Europea, es que sea efectivo en el mundo de los big data, sabiendo que esto va a cambiar dentro de 20 años, aun cuando nosotros hoy hagamos una propuesta que llevará años de discusión y aplicación.

La legislación que estamos manejando hoy día, que entrará en vigor el año próximo, va a durar por lo menos 20 años, que es más de un siglo en términos digitales. Tenemos que considerar

---

las expectativas en el largo plazo. Mi visión es que pronto veremos la noción de los datos personales como algo que desaparecerá. Todos estaremos fácilmente identificables en el mundo de los big data. Esta noción del anónimo quedará solo en los libros. Hablamos de reglas, hablamos de principios, hablamos de multas administrativas y todo está bien pero qué pasa con las 25 disposiciones que están en el reglamento, en el GDPR, que permite a reguladores independientes expresar una única opinión y emitir directrices para certificar categorías de procesamiento o el procesamiento de datos personales.

Así tenemos un conjunto adicional de reglamentaciones inclusivas basadas en un proceso de consulta. Hay mucho espacio aquí para generar una mayor especificidad y también para ser inclusivos ya que ahora los reguladores independientes tendrán la oportunidad de interactuar con las partes interesadas pertinentes. Lo que puedo ofrecer a cambio es un marco jurídico más serio basado en determinaciones administrativas más armonizadas. La idea es expresar una única voz en un abordaje basado en la directiva de la Unión Europea de 1995, algo que va a desaparecer y se va a modificar. Estamos ofreciendo un sistema que va a ser complementado por la reglamentación de ePrivacy o privacidad electrónica, que es una legislación esencial para los controladores de datos que trabajan en las redes de comunicación privadas.

---

Estamos ofreciendo un sistema basado en disposiciones tecnológicamente neutrales. Queremos permitir que los controladores de datos que están establecidos fuera de la Unión Europea, que estén en terceros países, tengan un único número que codificar. Así comprometernos profundamente con otros controladores. Hablamos de asistencia recíproca y operaciones conjuntas. A los operadores que tienen interés en trabajar en más de un país, que sepan que no tienen que usar distintos abordajes con las autoridades. Nuestro abordaje está comprometido con el fortalecimiento de la cooperación internacional. En nuestro sitio web hay documentos de nuestro contacto con autoridades hermanas en el mundo y también con organizaciones internacionales.

Por último, quiero decir que la contribución europea al debate internacional sobre la protección de datos debería también ser completa y coherente. Que sea una respuesta a las crecientes preocupaciones acerca de la consistencia de este marco jurídico respecto de otras legislaciones tales como la legislación sobre derechos de autor, los derechos del consumidor y la iniciativa de la cámara compensadora digital lanzada por mi institución, la oficina del supervisor europeo de protección de datos.

No quiero dejar solos a los organismos de aplicación de la ley. La reglamentación GDPR es relevante para ustedes. Es una directiva que permite la cooperación entre las autoridades policiales y las

---

autoridades judiciales que debe ser implementada a nivel nacional por los estados miembros en mayo del año próximo. Es un medio en el cual los países europeos estarán más basados en los principios de proporcionalidad. Consideren lo que decía Caroline. Europol, INTERPOL y el FBI estarán sujetos a una nueva reglamentación que entrará en vigencia el 1 de mayo de este año. Mi institución en cooperación con otras instituciones internacionales estará cubierta por esta nueva reglamentación.

Tenemos mucho que considerar en esta dimensión global. Mi recomendación es que sí, hay que considerar la dimensión de la transferencia de los datos de la Unión Europea. Hemos oído hablar de este proyecto, de transferir los datos a VeriSign en los Estados Unidos pero, por favor, consideren, desde el punto de vista legal, centrándome en la disposición, el alcance de la aplicación del nuevo GDPR que se aplica no solo a la transferencia. La transferencia es una operación de procedimiento pero la reglamentación GDPR será aplicable en su totalidad a todas las operaciones, incluyendo la recopilación, la elaboración y la retención de los datos. Una compañía establecida en Japón o en los Estados Unidos estará sujeta al reglamento GDPR, independientemente de en qué momento se transfieran los datos fuera de la Unión Europea siempre que ofrezca servicios en la Unión Europea.

---

Aquí el punto clave será la localización de dónde se ofrecen los datos. Con respecto a la transferencia, aún no es clara la perspectiva del nivel de medidas de protección. Recientemente, el tribunal de justicia dijo que el principio de protección adecuada de datos personales significa después del tratado de Lisboa que las medidas de protección ofrecidas en un tercer país tienen que ser esencialmente equivalentes, y esto es algo que todos nosotros estamos analizando. Hay otros fallos o decisiones. Por ejemplo, el PNR canadiense que estableció que deben ser relevantes horizontalmente al igual que el famoso fallo sobre los Digital Rights vs. Irlanda, con respecto a los operadores de Internet que contiene consejos útiles para nosotros. Es un trabajo en curso pero también tenemos ya bastante claridad y mucha flexibilidad. Estamos todos entonces comprometidos a ocuparnos de nuestra legislación nacional pero con una perspectiva global porque la perspectiva o la respuesta necesariamente tiene que darse a nivel internacional.

THOMAS SCHNEIDER: Gracias, Giovanni. Ahora tenemos a Wilbert Tomesen, que es el vicepresidente del grupo de trabajo de Artículo 29.

WILBERT TOMESSEN: Muchas gracias. Al igual que Giovanni y otros colegas, nosotros nos podemos hacer eco de todo lo que ha señalado. Voy a ser

---

breve. Pensemos en una imagen que vi del presidente Obama en el primer piso. Recuerdo que se lo citó diciendo: “No se les estoy trayendo temor. Les estoy trayendo el futuro”. Eso es cierto. Nosotros en Europa no estamos viviendo en una lista. Obviamente que no. también hablamos de privacidad y protección de datos. Es algo que tiene que ver con lo que está pasando en el mundo. Hemos estado también llevándolo, incorporándolo a las leyes reales y hemos otorgado facultades de aplicabilidad de estas leyes, DPA con facultades de aplicar sanciones, pero esto nos lleva nuevamente al meollo del asunto.

Tiene que ver con un mundo que se basa en datos en el que estamos viviendo hoy. Si pensamos en cómo se manejan esos datos de cara al futuro, estoy sumamente convencido de la necesidad de hacer de manera equitativa, de manera transparente y también de manera previsible el manejo de esos datos. Tenemos el aniversario número 28 de la invención de Internet. Como dijo Tim Berners-Lee, no hemos perdido el control de nuestros datos personales pero eso es lo que estamos tratando de evitar en Europa. Si esto es así, nos preguntamos: ¿Cómo los podemos recuperar?

Estamos hablando de tener facultades para aplicar las leyes, para aplicar sanciones pero por qué estamos recabando datos. Creo que ese es el interrogante que uno se tiene que hacer. ¿Para qué se están recabando estos datos? ¿Cuál es la finalidad?

---

¿Cómo se asegura un uso transparente de los datos para que no infrinja las leyes? Como dijo Giovanni, nosotros vemos que es nuestro deber asistirlos a ustedes cuando es necesario dar respuesta a estos interrogantes asociados tan difíciles. Los principios no son tan difíciles. Hay que preguntarse por qué lo estoy haciendo. ¿Puedo hacerlo? ¿Estoy siendo justo? Muchas gracias.

THOMAS SCHNEIDER: Gracias. Muy bien. Tenemos tiempo entonces, espero, para un intercambio interactivo. Le quisiera dar la palabra a los miembros del GAC para que formulen sus preguntas o sus comentarios. Esperemos tener un buen debate. Países Bajos, por favor. Preséntense, por favor, porque algunos no los conocen.

PAÍSES BAJOS: Muchas gracias, señor Presidente. Soy Thomas de Haan, del Ministerio holandés de Asuntos Económicos, representante de Países Bajos en el GAC. Tengo una pregunta para el señor Buttarelli. Realmente me complace mucho que en esta sesión usted expresara aquí que quieren hacer esta contribución del lado europeo para la interpretación del nuevo reglamento para el próximo año. Quisiera remitirme a la sesión anterior que creo que fue sumamente positiva. Muchas personas de la comunidad expresaron sus opiniones y los felicitamos también por todo el

---

trabajo hecho y su voluntad de asistir a la ICANN en el ámbito de la privacidad. Creo que nosotros en el GAC somos quienes nos preocupamos más por los intereses de naturaleza pública de nuestros ciudadanos dentro de la ICANN y somos muy conscientes de las posibles infracciones, violaciones que podrían producirse. Pensamos siempre en cuáles son los ámbitos de aplicación de los contratos de la ICANN con los registros, los registradores.

Quiero volver entonces a esa sesión anterior donde se hizo referencia a lo que se incorporó en el acuerdo de registro que ha sido firmado para varios de los nuevos gTLD. Recuerdo que muchos de esos gTLD fueron concedidos a través de este concepto de .BERLIN en Europa. Ahora hay muchos de estos nuevos en Europa. También tenemos .AMSTERDAM, .FRL. Somos conscientes de la urgencia de incorporar esas dos cláusulas. No estoy hablando de la transferencia de datos sino de la publicación de los datos y de las maneras que ya nos dan problemas. Hay dos cláusulas que hay que cumplir de acuerdo a las leyes nacionales para presentar los datos.

Quisiera preguntarles si hay alguna posibilidad de que antes de que entre en vigencia el reglamento europeo de protección de datos, si del lado europeo se puede brindar cierta claridad con respecto a si esa implementación está en consonancia con este reglamento, el GDPR. La ICANN podría tener suficiente tiempo



---

para hacer las modificaciones que corresponda en los contratos. Tal vez esta es una pregunta más para la ICANN. Insto a la ICANN a suspender el cumplimiento sobre la base del contrato antiguo. Gracias. Esta es mi pregunta.

GIOVANNI BUTTARELLI: Estoy hablando también en nombre de Wilbert. Creo que la implementación del GDPR no se puede improvisar. Estos 14 meses hay que utilizarlos de la manera adecuada. Nosotros estamos encantados con el sistema de la ICANN y quisiéramos ayudarlos a poner en consonancia los objetivos con las novedades desde el punto de vista legislativo. No tenemos alternativa. Este reglamento, el GDPR, es simplemente una transposición de una obligación legal contenida en el artículo 16 del tratado sobre el funcionamiento de la Unión Europea de acuerdo al cual la protección de datos ahora es algo como un derecho fundamental separado de la privacidad.

Los datos son procesados por alguien. Aunque esa recolección de datos sea obligatoria, aunque tengan que publicarlos y tengan que estar disponibles a nivel del público, todo esto es parte de un derecho fundamental. Está sujeto a un escrutinio desde una base legal, como está mencionado en el tratado. Esto está en la constitución de la Unión Europea. Esta es una novedad que hay que considerar.

---

Permítame hacer referencia a otro ejemplo que parecía que no tenía solución hace un par de años: el sistema de WADA, que se utilizaba para antidopaje. Empezaron a recopilar información y se identificó luego la solución con éxito porque no somos expertos en el trabajo que realizan ustedes pero sí podemos ayudar a traducir toda esta legislación a la práctica. ¿Pero qué pasa con la flexibilidad y la honestidad? En primer lugar, la finalidad. La disponibilidad para identificar el medio menos invasivo para lograr esos propósitos o esa finalidad y abstenerse de cualquier publicación que no sea necesaria. ¿Cuál es la definición de necesario y la distinción de aquello que es útil? ¿Qué es necesario para los registros, para los registradores y qué es útil para los terceros, por ejemplo, desde el punto de vista de los organismos encargados del cumplimiento de la ley y los derechos de propiedad intelectual?

Hay que ser honestos y flexibles. Tal vez de esta manera, con las autoridades de protección de datos, podamos ayudar a transformar, a traducir estos principios en algo práctico. Tenemos ahora esta posibilidad para poder resolver algo que tal vez se presente dentro de 24 meses. Si alguien plantea una queja o un DPA, comienza una acción ex officio. Queremos evitar ese tipo de situaciones. Por eso en nombre de los otros colegas nos tomamos la libertad hoy en el almuerzo, con los miembros de la junta directiva de la ICANN, de sugerir que tal vez algunos de

---

ustedes podrían abordar a las autoridades encargadas de la protección de datos para que les brinden asistencia y nos pueden permitir a nosotros ayudarlos. Hoy no podemos resolver todos los problemas aquí en un panel, por supuesto. Simplemente podemos confirmar nuestra disponibilidad para ayudarlos.

WILBERT TOMESSEN:

Tal vez yo podría agregar algo. Básicamente, tenemos la forma en que nosotros presentamos. ¿Cómo informamos esos datos? Eso es lo que tal vez deberíamos preguntarnos. ¿Somos concisos? ¿Lo hacemos de manera comprensible? ¿Saben las personas lo que les estamos pidiendo y por qué? Estoy aquí en una situación en la que no solamente puedo dar respuestas que son favorables pero ustedes pueden explicarles a sus ciudadanos, a las personas que representan por qué están procesando esos datos, cuál es el motivo. ¿Pueden ser concisos y claros al respecto? Tal vez tengan que contratar a otro experto en comunicaciones pero dejar de procesar esos datos, esa también sería una opción, además de lo que Giovanni dijo con tanta razón. Si el procesamiento de los datos no puede incorporarse al marco de nuestras leyes futuras, que básicamente es una codificación de los principios que hemos conocido en todos estos años. Si no se puede incorporar a ese marco, me temo que tienen que detener esas actividades de

---

procesamiento. A fin de cuentas, esos son los principios, esas son las leyes. Tiene que haber claridad. Tienen que poder explicarlas y tienen que estar dentro del contexto del GDPR.

THOMAS SCHNEIDER: Gracias. ¿Hay más preguntas o comentarios? Adelante, Bélgica.

BÉLGICA: Gracias, señor Presidente. Buenas tardes a todos. Soy representante de Bélgica ante el GAC. También soy miembro de la Comisión de Privacidad de Bélgica. Este no es un tema nuevo, por supuesto. Hace años que hablamos de la protección de datos dentro del GAC. Por eso es que celebro que estén aquí hoy y que tengamos hoy esta oportunidad de pedirles ayuda para esclarecer algunas cuestiones. Lo que yo quisiera saber es si ya han interactuado con ICANN porque nosotros les enviamos consejos. A veces nos escuchan, aunque no siempre. La idea sería entonces definir en nuestros consejos cuáles serían los grandes principios comunes entre todos los países miembros del GAC para recordarles los principios básicos en materia de protección de datos y de privacidad, sobre todo.

Para nosotros, sería muy productivo que ustedes pudieran identificar cuáles son para ustedes las disposiciones que podrían ser contrarias a los grandes principios y que están presentes en

---

los contratos, como decía mi colega holandés, contratos de registro con ICANN. Quisiera preguntarles también si han tenido interacciones productivas con ICANN. Gracias.

THOMAS SCHNEIDER: Gracias, Bélgica. ¿Quieren dar una respuesta?

GIOVANNI BUTTARELLI: Todavía no podemos dar una respuesta. Estamos esperando algunas respuestas positivas. Mi predecesor envió hace unos años una carta sobre el tema de la retención de datos y ninguna de las sugerencias que hicimos fueron tomadas en cuenta. Aprobamos una opinión, un dictamen hace 14 años dentro del grupo de trabajo del artículo 29. Se han hecho comentarios pero todavía estamos esperando un resultado positivo. En el 2013 junto con otras autoridades de la Unión Europea aprobamos el dictamen 3 de 2013 sobre limitaciones con una finalidad que es sumamente pertinente para ustedes y puede ser de utilidad. Igualmente hoy estamos comenzando a hablar de estas discusiones pertinentes.

Seguimos estando a su disposición. A título informativo, permítanme decirles que EDPS, los supervisores de protección de datos de Europa, junto con los coanfitriones que rotan, cada dos años organizan un evento para las organizaciones y

---

entidades internacionales que no están sometidas a las cláusulas en materia de protección de datos. Aquí estamos teniendo en cuenta los deberes de la ICANN en términos generales como entidad y también los deberes y obligaciones de los controladores de datos únicos que siguen las políticas de la ICANN. En caso de que a la ICANN le interese sumarse a nosotros, por favor, tengan en cuenta que a principios de mayo realizaremos el próximo evento en Ginebra. Creo que son los días 11 y 12. Todos los detalles están en el sitio web de mi organización. Con gusto vamos a recibirlos. Allí verán cómo otras organizaciones internacionales que no están sujetas a las leyes nacionales comparten experiencias en términos de implementación. Esto da lugar a la creatividad para entender lo que otros están haciendo. No se toman decisiones. Es simplemente un momento de intercambio y de compartir, y saber qué es lo que están haciendo otros.

THOMAS SCHNEIDER: Gracias. Antes de darle la palabra a Tarek quiero decir que la junta directiva ha dado señales de que está interesado en trabajar con los comisarios a cargo de protección de datos. Ya han tenido este almuerzo, como ustedes dijeron, en el día de hoy. Este es el comienzo de un intercambio un poco más regular, más periódico que el que tuvimos en los últimos años. Como ya se dijo en la sesión, hubo algunos contactos pero no fueron tan

---

productivos. Le voy a dar la palabra a Tarek, de la ICANN, quien tal vez haga referencia a la respuesta de la junta directiva.

TAREK KAMEL:

Exactamente. Iba a decir eso. Tuvimos una reunión constructiva con la junta directiva y el presidente Steve Crocker. Dio claras señales en nombre de la junta directiva de que recibían con agrado la presencia de los comisarios en esta materia y que este era el comienzo de un diálogo constructivo y de un trabajo conjunto con la comunidad, con la junta directiva y las distintas unidades constitutivas, la GNSO, el GAC, para avanzar en esta materia. Creo que va a haber también pasos y medidas concretas del lado de la ICANN. La ICANN rápidamente va a responder a las reflexiones tan positivas que surgieron de la reunión de hoy con la Comisión Europea y el Consejo de Europa. Gracias, Thomas, por brindarme la oportunidad de reconfirmar esto. No vamos a esperar otros 14 años para que ocurra algo.

THOMAS SCHNEIDER:

Gracias. Giovanni.

GIOVANNI BUTTARELLI:

En nombre de Wilbert, por compromisos conflictivos, Wilbert y yo tal vez somos los únicos que quedamos en el panel que estamos obligados a salir para el aeropuerto en 10 minutos. Si

---

hay espacio para uno o dos preguntas más, con gusto las responderemos, de lo contrario, ya les pido disculpas de antemano porque vamos a tener que retirarnos.

THOMAS SCHNEIDER: Rusia.

RUSIA: Es una pregunta para Alessandra. O tal vez no sea una pregunta y sea una propuesta. Al comienzo de su intervención habló de un informe del Consejo de Europa sobre derechos humanos en los nuevos gTLD. Nosotros el sábado hablamos de este informe. Fue un informe muy útil y que ya está disponible. Es muy valioso. Allí nos da conocimiento de expertos externos. ¿Cómo podemos planificar el mismo tipo de trabajo desde el punto de vista de la protección de datos personales en los procedimientos de la ICANN? Si no se puede planificar, tal vez la propuesta sería pensar en hacer un análisis de ese tipo. Creo que sería un instrumento de mucho apoyo para nosotros porque trabajo un poco la protección de datos personales y privacidad, y también la protección en el ámbito digital y este es un tema muy complejo. Todo análisis externo, independiente de expertos puede ser de utilidad porque nos agrega otro punto de vista. Siempre eso es muy útil.



---

THOMAS SCHNEIDER: Johannes.

JOHANNES KLEIJSSSEN: De hecho, yo fui el que mencioné este informe. Gracias por el intercambio de opiniones hoy, basadas en la propuesta respaldada por las distintas comunidades de ICANN. Nos interesará mucho presentar un informe al GAC sobre los distintos aspectos de la protección de datos dentro de ICANN y las reacciones que hemos recibido hasta ahora son alentadoras en ese sentido. Lo esperamos con mucho gusto. Gracias.

ALESSANDRA PIERUCCI: Quizá para complementar. Quiero asegurarles que estos debates han sido reportados al comité consultivo. De hecho hace años que venimos siguiendo el trabajo de ICANN. Es constante la comunicación que ha existido con los miembros del comité consultivo así que muchas gracias por su propuesta. Gracias.

THOMAS SCHNEIDER: Para aquellos que no recuerdan, el Consejo de Europa encargó un informe sobre derechos humanos y nuevos gTLD. No TLD de comunidad sino derechos humanos y los nuevos TLD en 2014 que se ocupaban de la libertad de expresión y la libertad de

---

reunión junto con protección de datos. Yo fui uno de los coautores. Si leen el informe, es del 2014. Si no lo tienen, yo ya ni lo encuentro, o si es que no estaban en esa época en el GAC, podemos organizar que tengan una copia. Gracias. ¿Algún otro comentario o pregunta? Sí, Cathrin.

CATHRIN BAUER-BULST: Cathrin Bauer-Bulst, de la Comisión Europea. Gracias, Thomas. Yo también tengo el honor de ser copresidenta del grupo de seguridad pública del GAC. Quiero hablar del hecho de que los organismos de protección de la ley y protección de datos en el pasado no se reunían. Aquí en el GAC hemos trabajado con mucho éxito en esta coordinación y hay mucho interés en las comunidades de protección de datos y aplicación de la ley respecto de la exactitud de los datos disponibles para impedir el uso indebido de los datos. Les aliento a que vean que en el grupo de trabajo sobre seguridad pública trabajamos mucho en estos conceptos. Intentamos crear un sistema que a la vez dé cabida a los intereses legítimos de lo que es aplicación de la ley, tanto civiles como penales y a la vez se centre en la protección de los derechos humanos, el derecho a la vida, el derecho a la dignidad humana, coordinado con el interés legítimo de la protección de datos.

---

Tenemos varias presentaciones sobre los principios de protección de datos y cómo pueden utilizarse en el nuevo proceso de desarrollo de políticas, el sistema RDS nuevo. Les aliento a que analicen la perspectiva de la Comisión Europea y del grupo de trabajo de seguridad pública, que es la de participar activamente en estos procesos estando aquí presentes y hablando también en los PDP. Para nosotros es sumamente difícil traducir estos principios abstractos tales como la limitación de propósito y conseguir una definición apropiada de lo que es propósito y algo que pueda trabajarse en una política aquí en ICANN.

En lo personal, yo identifico sinergias posibles de incorporar estos principios y traducirlos en un marco trabajable que no ha venido pasando por la desconexión entre las posiciones adoptadas desde afuera y el trabajo que se da aquí adentro. No puedo más que alentarlos a que se involucren más y continúen participando en el grupo de trabajo sobre seguridad pública y en los PDP. Gracias.

THOMAS SCHNEIDER: Gracias. ¿Algún otro comentario o pregunta? Sí. La EBU.

---

UNIÓN DE RADIODIFUSIÓN EUROPEA:

Muchas gracias por darme la palabra. Tengo una pregunta para el profesor Cannataci. Esa visión pesimista de que en el mundo de los big data sería casi imposible o imposible mantener nuestros secretos de lo que hacemos. ¿Usted comparte esta visión o piensa que será algo manejable y que no ocurrirá de esta manera?

JOSEPH CANNATACI:

Esta no va a ser la respuesta de un abogado. La respuesta será sí y no. a ver. Primero quiero hacer una introducción. Quiero recordarles a los colegas en la sala que con la camiseta de relator especial tengo varias tareas. Tengo un grupo de trabajo que se ocupa de distintas cosas. Una de ellas es big data y open data, que son una de mis prioridades. Big data y open data es una de las áreas sobre las que espero poder presentar un informe entre el mes de julio y octubre de este año.

Habiendo hecho esta introducción, con este contexto, es un tema a tratar con cuidado. Todos hablan del big data. El Consejo de Europa acaba de emitir una directriz el viernes pasado. La Comisión de Información del Reino Unido también publicó un nuevo informe. Estamos trabajando a nivel de Naciones Unidas también. Yo creo que el pesimismo, si es que existe, francamente Giovanni estaba siendo más realista que pesimista. Depende de

---

qué es lo que vamos a hacer respecto de otra cosa. Creo que es incorrecto hablar de big data. Creo que cuando hablamos de big data también tendríamos que hablar de otras dos cosas. Sin duda, una. La primera es open data, datos abiertos.

Big data no puede ser tal amenaza a la privacidad a menos que los abordajes analíticos del big data también recurran a otros conjuntos de datos. En especial, lo que tenemos que considerar aquí son aquellos conjuntos de datos que se ponen en el dominio público por parte de autoridades públicas que son las que originalmente recopilaron esos datos. En muchas jurisdicciones del mundo hay bases de datos, el seguro social, las bases de datos de salud que se recopilan para un propósito, y hay otros que encuentran estos datos y dicen: “Muy bien. Podemos darle un gran beneficio a la humanidad si pasamos estos datos al dominio público”.

No voy a hablar de este argumento, del beneficio para la humanidad. Obviamente, en tanto una compañía privada empieza a aprovechar esos datos que han sido trasladados al dominio público, la primera línea de procesamiento pasa a lo que es propiedad intelectual. Esto es algo que parece ser olvidado por muchas personas que han estado haciendo lobbying activo a favor de esto o que están del lado de los gobiernos que no lo logran ver o que quizá sí lo ven.

---

En realidad, yo creo que si uno se queda con el principio original, el propósito para el cual se recopilaron los datos, estos datos no debieran ser divulgados para ningún otro propósito. No debieran divulgarse grandes cantidades de datos en el ecosistema abierto a menos que se tenga un motivo por ser menos pesimista. Además, en niveles cada vez más crecientes, por la forma en que se van aplicando las leyes en el mundo, esa parte de la protección de datos esperamos que sea más efectiva. Digo esperamos porque en mi opinión el GDPR es una de las grandes áreas grises. Desde el punto de vista estadístico, para investigación, hay un elemento de delegación a las autoridades nacionales en lugar de tener un abordaje regulatorio de nivel superior.

Si vamos a repensar qué es big data y open data, y refinamos el análisis, deberíamos ser menos pesimistas pero hay mucha presión de muchas áreas por parte de muchos políticos para decir que sí a lo que es big data y open data. Yo sé que en los últimos 18 meses he visto países que incluso en pequeños pueblos o pequeñas ciudades, en países relativamente pequeños, más pequeños que Dinamarca, big data se consideró una enorme y positiva gran herramienta para servicios sociales. Eso, la verdad, puede funcionar para trabajadores sociales en pequeñas ciudades pero para eso no se necesita big data. Se necesita un mejor abordaje del sistema de jubilaciones, por

---

ejemplo. La cantidad de argumentos tontos en defensa de lo que es big data y de open data es increíble. Parece que la gente lo cree y eso a mí me hace preguntarme por qué.

No hay duda de que las herramientas analíticas de big data sin duda pueden ser utilizadas en provecho de la humanidad. Por ejemplo, en el área de salud. Pero hay que manejarlo con mucho cuidado. Espero que en los próximos años veamos más investigación sobre este tema. Así podremos responder con una actitud más positiva a su pregunta. Gracias.

THOMAS SCHNEIDER: Muchas gracias. Alessandra, ¿quiere decir algo al respecto?

ALESSANDRA PIERUCCI: Sí, una información adicional y hacerme eco de lo que se viene diciendo. Por supuesto, big data introduce retos que son difíciles de resolver. El Consejo de Europa, como decía Joe, de hecho el comité consultivo adoptó directrices a comienzos de enero sobre big data donde básicamente reconoce el hecho de que si bien el principio tradicional de protección de datos se ve cuestionado, el consentimiento informado incluso el principio del propósito, de alguna manera las directrices alientan a los legisladores a salir de la noción tradicional del control individual de sus datos personales y optar por un abordaje diferente. Digamos, una

---

evaluación de impacto múltiple de los riesgos de big data, lo cual les asigna mucha responsabilidad a quienes operan big data y también en términos de la evaluación del aspecto ético detrás de lo que es big data. Gracias.

THOMAS SCHNEIDER: Sí. Caroline.

CAROLINE GOEMANS-DORNY: Sí. En el futuro, con respecto a big data como dijimos en otros paneles, el abordaje tecnológico será muy importante. La tecnología es neutral pero se la puede usar en ambos sentidos. No es per se una tecnología intrusiva para la privacidad. También puede mejorar la privacidad. Por ejemplo, si vemos los primeros escáneres de imagen en los aeropuertos para la seguridad de los pasajeros, los primeros eran terribles. Eran muy controversiales. Ahora se instalaron filtros de privacidad. Los detalles del cuerpo se difuminan. Los elementos peligrosos se resaltan. Con eso se consigue la misma funcionalidad, la seguridad, que es el propósito, la seguridad de los pasajeros que suben a la cabina pero la tecnología se ha adaptado y es muy importante tener esta mentalidad de que la tecnología puede mejorar la privacidad.



---

THOMAS SCHNEIDER: Gracias. ¿Alguna otra pregunta o comentario? de no haber, no cabe duda de que el día ha sido para todos muy largo y muy interesante. Como dije en la reunión previa, como también soy responsable de la organización de la parte suiza del IGF en Ginebra, creo que este es uno de los temas que estará en el foco de la atención en Ginebra. No solo los temas de la ICANN específicamente. Dada la cantidad de talleres que habrá, será una opción. Si algún representante del mundo comercial de la ICANN al igual que otras partes interesadas hace una propuesta para discutir un tema, eso se puede acelerar para encontrar soluciones para los aspectos relacionados con ICANN de este desafío y también de otros desafíos más amplios relacionados con lo que es big data y privacidad en general. Sin duda serán discutidos en varias ocasiones en Ginebra.

Con esto, quiero agradecer nuevamente al Consejo de Europa y, por supuesto, a ustedes en lo personal por haberse acercado aquí. A la INTERPOL. Espero que hayan disfrutado de la tarde. Para aquellos que puedan quedarse, está el evento de la gala no muy lejos de aquí, en el mismo enorme edificio en que estamos. Aquellos que todavía no han recibido la invitación, espero que la podamos manejar porque ni siquiera yo la tengo. No la pude conseguir. Gracias y nos vemos después en el otro lado del edificio. Gracias. Gracias a ICANN por haber facilitado la sesión.

**[FIN DE LA TRANSCRIPCIÓN]**