México, D.F., 13 de noviembre de 2014.

Versión estenográfica de la Sesión 7. "Las nuevas tecnologías en la protección de datos", durante el XII Encuentro Iberoamericano de Protección de Datos Personales, llevado a cabo en el Auditorio "Alonso Lujambio" del Instituto Federal de Acceso a la Información (IFAI).

Presentador: Con estas jornadas en el Décimo Segundo Encuentro Iberoamericano de Protección de Datos Personales, damos inicio a la Sesión número 7, denominada "Las nuevas tecnologías en la protección de datos".

Modera esta mesa el Comisionado del IFAI, Oscar Guerra Ford, quien tiene el uso de la palabra.

Óscar Mauricio Guerra Ford: Muy buenas tardes.

Bienvenidos a esta última mesa de este Encuentro Iberoamericano de Datos Personales.

Voy a ser muy breve y parco en las intervenciones, como moderador.

Voy a moderar simplemente por el número de panelistas, la hora y poder también respetar los tiempos para la Ceremonia de Clausura.

En esta Sesión se analizarán algunos de los retos más importantes que enfrenta el derecho a la protección de datos personales, frente a las nuevas herramientas tecnológicas, las personas que nos acompañan, que son seis, probablemente se sume Danilo, que viene en camino, sin que sea verso, del Aeropuerto, y entonces serán siete, por lo cual el tiempo de exposición de cada uno, así lo habíamos acordado, será de 10 minutos, con una segunda ronda de tres, y si no llegara Danilo, esperamos que sí, se les podrá alargar hasta cinco minutos y les pedimos que seamos todos respetuosos con el tiempo, y si no, pues será mi labor en esa materia.

Bueno, pues obviamente a nombre del IFAI, agradezco la presencia de todos los que nos acompañan en este Auditorio doctor Lujambio y

obviamente de los compañeros panelistas que los voy a presentar a cada uno en el orden de su intervención y así les iré dando la palabra.

Vamos a iniciar con la doctora en derecho y ciencias políticas, Ana Brian, quien nos visita del Uruguay, quien es socia activa del Colegio de Abogados de Uruguay.

Dentro de su experiencia se encuentra, que desde 1992 se ha desempeñado como asesora legal del Parlamento de Uruguay, es profesora de derecho informático en la Universidad de la República Oriental del Uruguay, consultora principal del estudio jurídico Brian and Associates y del Colegio de Abogados de Uruguay.

Además es miembro de diversos Foros Internacionales sobre protección de datos, como la Red Iberoamericana de Protección de Datos, el grupo de trabajo internacional sobre la protección de datos en las telecomunicaciones y de la Asociación Internacional de Profesionales en Privacidad.

De verdad agradecemos la presencia de Ana y te damos la palabra.

Ana Brian Nougreres: Gracias, Óscar.

En primer lugar quiero agradecer al IFAI y a los señores comisionados, así como a las autoridades de al Re Iberoamericana de Protección de Datos y del encuentro, la posibilidad que me dieron de estar aquí hoy presente compartiendo con ustedes estos minutos y algunos conceptos. Es para mí un honor poder estar hoy acá.

Dicho esto, no quiero dejar de tomar 30 segundos para resaltar lo enriquecedoras que han sido los distintos paneles y las distintas ponencias presentadas que han sido fruto de discusiones de pasillo numerosas y que creo todos nos vamos a ir más ricos en conocimientos y con más cosas para discutir de aquí. Muchas gracias.

Dicho esto y entrando al tema de las tecnologías al servicio de la protección de datos, me voy a referir a lo que es un ejemplo de cómo aplicar las nuevas tecnologías de la protección de datos, para la protección de datos en especial, a la rutina del Privacy by Design.

¿Por qué me refiero a la doctrina del Privacy by Design? Porque es una doctrina que ha tenido muchos reconocimientos a niveles varios, es una forma de encausar la protección de datos tecnológicamente como hay muchas otras.

¿Por qué me refiero a esto? Porque desde el año 2010 que ha tenido menciones especiales, por ejemplo, en la Conferencia de Protección de Datos de Jerusalén, con respecto a la importancia de la teoría se reconoció que es un componente que tiene que ver con los fundamentos de la protección de datos.

Asimismo, en el 2011 en foros que tienen más relación con la parte de ingeniería y de seguridad de la información, tuvo sus reconocimientos y también a nivel de Estados Unidos tuvo reconocimientos, es más, la primera vez que se utilizó el término Privacy by Design, fue en Estados Unidos de Norteamérica por los senadores Kerry y McCain.

De ahí en más, estos son sólo ejemplos, pero de ahí en más hasta el día de hoy en la declaración de Mauricio se pueden ver las recomendaciones de que se sigan aplicando los principio de la teoría del Privacy by Design.

¿En qué consiste básicamente esto? El primer concepto está dado por el Smart Privacy o la privacidad inteligente de la cual es un ejemplo en la gráfica que pueden ver. Lo que se hace es considerar primero lo que son las bases, la parte sobre la cual se funda toda la teoría, que está primariamente por lo que son las prácticas justas para el tratamiento de la información.

Luego de considerar todo lo que tiene que ver con las prácticas justas y adecuadas para el tratamiento de la información y de los datos, se comienza hablar de la seguridad de los datos. Y ahí están dadas la base de lo que es la construcción de *“Privacy by Design”*, para el tratamiento de la información y de los datos, se comienza a hablar de la seguridad de los datos.

Y allí está dada la base de lo que es la construcción del *“Privacy by Design”*, que tiene cinco pilares. Los pilares son todos los elementos de los que hemos hablado hasta ahora, lo que tiene que ver con educación, lo que tiene que ver con concientización, lo que tiene que

ver con las fuerzas del merado también, con necesidad de auditorías, con practicar la transparencia en lo que son las formas de instrumentar la protección de datos y la privacidad.

¿Cuáles son los principios que inspiran la protección de datos personales conforme a este concepto?

Bueno, básicamente los mismos que vemos en todos lados, consentimiento, rendición de cuentas. Solamente los voy a mencionar, así tomamos los tiempos que necesitamos y nada más y ustedes van a ver que son los mismos que familiarmente encontramos en todos los ordenamientos.

Finalidad, limitaciones en la colecta, minimalización, uso, retención y acceso limitados, principio de la proporción, exactitud, principio de veracidad.

En cuanto a seguridad, en la seguridad se atiende desde el punto de vista físico, técnico y administrativo; todo lo que tiene que ver con transparencia, acceso y conformidad.

¿En qué consiste entonces la Teoría de *“Privacy by Design?*

Consiste en que la privacidad se muestra dentro de lo que es la arquitectura del sistema.

Cuando se inicia un emprendimiento empresarial, se trata en el momento que se implementa el armado del modelo de negocios, cuando esto se lleva a una implementación técnica, informática, se implementa la *“privacy”,* o sea, la protección de datos dentro de lo que es la arquitectura y el diseño físico de la red, de forma tal que queda dentro del sistema mismo.

Este es el sistema original, o sea, la implementación desde el nacimiento del negocio.

Hoy por hoy ya hay muchos casos que refieren a *“Privacy by Design”.*

¿Qué significa esto?

Que una vez que el negocio ya está implementado, que la empresa ya está funcionando, bueno, se ve la forma de poder implementar el sistema de protección de datos.

¿Cuáles son los siete principios fundacionales del *“Privacy by Design?*

El primer principio tiene que ver con que no se trata de una forma de actuar reactiva, sino que es proactiva.

O sea, más allá de que es necesaria la regulación y demás, aquí a lo que vamos es a la cuestión práctica. O sea, se trata de utilizar proactivamente los conceptos que tenemos de cómo debe implementarse la protección de datos y la privacidad en todo lo que es el negocio y la arquitectura de la red.

El negocio siguiente tiene que ver con que la privacidad debe funcionar por defecto. O sea, se van a pedir los datos necesarios, ni más, ni menos. Y todo eso va a estar en el sistema ya implementado.

Cuando nos acercamos en una empresa a la recepcionista y ella nos va a pedir algunos datos. Bueno, ese sistema que ella tiene y que ella maneja en ese momento no va a permitir que el usuario se confunda y no va a permitir que pida más datos que los necesarios, ni datos diferentes de lo que son estrictamente para el caso en cuestión. O sea, la privacidad actúa por defecto.

La privacidad, como les decía, se muestra dentro de lo que es el diseño del sistema. O sea, está dentro de la arquitectura de red del sistema y funciona plenamente en un esquema ganar-ganar. O sea, no tenemos una contradicción como diciendo vamos a implementar la privacidad, pero acá tenemos que cotejar con otros. No, no.

Plenamente se está utilizando en forma tal que no haya que hacer un contralor o un límite, por qué, porque ya está dentro del sistema. O sea el sistema muestra toda su potencialidad de forma que la privacidad esté protegida.

La seguridad se muestra durante todo el ciclo vital del dato, o sea, va desde la colecta, pasa por todos los tipos de archivo que puedan implementarse en el medio y termina cuando se hace el delibery del

dato. Durante todo el ciclo vital del archivo, etcétera, está presente la seguridad de la información.

El principio seis refiere a visibilidad y transparencia. Se trata de que el proceso por el cual se trata el dato sea absoluta y totalmente visible y transparente para todo quien quiera y pueda interesarse en el mismo.

El principio siete refiere al respeto por la privacidad de los usuarios, o sea en lo que tiene que ver concretamente con un usuario que se presenta, bueno, la opción es siempre hacia la privacidad. No se va a privilegiar otros derechos, sino ese derecho se va a entender como fundamental.

¿Cómo funciona esto de los hechos? funciona con la triada, tecnologías de la información, modelos de negocios y estructura física e infraestructura de la red o sea la arquitectura de la red, y alrededor todos los elementos que manejamos. Pro-actividad, privacidad por defecto, privacidad embebida en el diseño, la funcionalidad ganar-ganar.

Protección durante todo el ciclo vital, enfoque centrado en el usuario y visibilidad y transparencia.

Por último y de manera complementaria para asegurar un sistema que sea exitoso es necesario hacer frecuentemente. O sea, manejar herramientas que nos puedan permitir analizar lo que son riesgos potenciales del sistema que está en funcionamiento.

Gracias, es todo.

Óscar Guerra Ford: Muchas gracias, Ana. Gracias, de verdad, por ajustarte al tiempo. No voy a resaltar, creo que es una exposición muy interesante que habla de otro tipo o de un modelo, no novedoso, pero que también es importante traer en este encuentro.

Voy a dar ahora uso de la palabra a la maestra Lina Ornelas, quien actualmente, como todos sabemos es la Jefa de Políticas Públicas y Relaciones con Gobierno para México, Centroamérica y el Caribe de Google.

Ella cuenta con más de 12 años de experiencia en el sector público y en México y en Europa. Fue Coordinadora de Subgrupos de Trabajo en la Red Iberoamericana de Protección de Datos Personales. Es miembro del Consejo Editorial de Futuro y Privacy Forum, y es miembro de la Asociación Internacional de Profesionales de Privacidad.

Forma parte del Consejo Asesor de México y en el instituto de la Fundación Wilson, en Washington, y además de haber publicado libros y numerosos artículos en materia de protección de datos personales. Pues como todos sabemos ha sido y fue por mucho tiempo una importante funcionaria en el IFAI. Le tocó toda la parte de la elaboración de la Ley de Datos Personales en Posesión de Particulares, los lineamientos y la protección de datos personales para ser sujetos obligados y fue asesora de muchas leyes, también de datos personales en diversas entidades, yo lo digo, lo fue en el Distrito Federal, entre otros.

Lina, como siempre, de verdad agradecemos tu participación en este encuentro, del cual ha sido parte de esta Red, y obviamente pues en el IFAI, que ha sido, fue pero siempre será tu casa.

Lina Ornelas Núñez: Muchísimas gracias, Oscar, y de verdad para mí es un honor estar aquí en el IFAI, que fue mi casa por nueve años, y sobre todo para poder compartir con ustedes desde este lado, cómo vemos las cosas en tiempos de la era digital, y en el tema de la protección de datos.

Y sobre todo estar con este panel de primera.

Me voy a remitir al tiempo que nos han dado, y bueno, el tema de esta Mesa es justamente cómo la tecnología puede servir para proteger mejor los datos.

Obviamente el uso extensivo de la tecnología y la espiral imparable de innovación, pues trae este manejo, digamos, de ingentes cantidades de información, pero también tenemos que tener claridad, respecto de que la misma tecnología nos presta por ejemplo mecanismos de encripción, de poder tener disponibilidad de la información en caso de pérdida, en fin.

En la industria se han desarrollado las mejores prácticas, en Google nosotros buscamos proteger siempre los datos de los usuarios.

Por ejemplo, contra fishing, contra virus, contra mileware, spamers y otros mecanismos que permiten que se robe la información. Y como les dije, hay muchísima disponibilidad de la misma y tenemos un grupo de ingenieros de alto nivel, los mejores ingenieros capacitados, cientos de ellos solamente abocados a los temas de la navegación segura para impedir la mala utilización de datos personales.

Pero creo que lo más importante es hablar de cómo empoderamos a los usuarios, al darles herramientas de control de su información, que desafortunadamente se desconocen por la mayoría de la gente y ahí necesitamos la educación como abordaje, porque la industria hace grandes esfuerzos, pero después no llegan al usuario final.

Por ejemplo, cuántos de ustedes utilizan Gmail, levanten la mano; cuántos de ustedes conocen el mecanismo de verificación en dos pasos para que su correo sea protegido. Entonces, esto tiene poco, pero muchísima gente que yo conozco, por ejemplo, no sabe que puede tener este pasword o contraseña.

Y bueno, hay muchas cosas que quisiera compartir en torno a eso, lo que se hace contra el fishing, cómo tenemos centros para proteger la actividad que tienen los usuarios, etcétera, y también en los dispositivos móviles, porque bueno, nació internet en lo que eran las computadoras en los hogares, pero desde los 80’s hay PC’s y ahora, pues tenemos el Internet, en un dispositivo móvil.

Entonces, tenemos también muchísimas cuestiones que no me voy a referir a ellas, porque son técnicas, pero que ustedes pueden consultar de cómo pueden tener control desde su teléfono, etcétera y cómo hemos construido o tratado de construir una internet más segura a través de alianzas con la sociedad civil, y también nuestros reportes de transparencia, etcétera, en donde ustedes tienen el control de su información en todas partes.

Finalmente hay un centro de protección para la navegación segura para las familias, en donde hay conversaciones que todos podemos emprender en torno a la seguridad.

Pero lo que yo quisiera es enfocarme rápidamente y necesariamente al tema que se abordó desde el principio en este Foro y a lo largo de estos dos días, sobre el derecho al olvido, porque está relacionado con cómo funcionan los motores de búsqueda y a los aspectos tecnológicos que desafortunadamente pues la sentencia del Tribunal Europeo… Bueno, primero quisiera decir que se trata de una resolución que Google cumplió desde el primer día, al día siguiente que se nos notificó, se creó un formulario para que todos los usuarios en Europa pudieran ejercer esta instrucción que dio la Corte y en ese sentido lo que quisiéramos es más bien abrir la discusión y celebramos que en nuestra región se abra la discusión y se pongan sobre la mesa todos los prismas que tiene este tema.

Sí quisiera decir que el Tribunal Europeo interpreta sólo lo que se le pregunta, efectivamente como se dijo en la primera mesa, pero que interpreta una directiva que es del 95, es una directiva predigital y no lo digo de manera peyorativa, sino porque es un hecho. Google nació en el 98, para que podamos dimensionar un poco cómo con reglas del 95 en el 2014 se está tratando de resolver una problemática que es real y que Google reconoce que existe, pero que nos entran muchas dudas y quisiéramos más bien ayuda de todos para poder cumplir mejor.

En ese sentido, creo que es muy importante conocer cómo funcionan los buscadores, porque luego hay a veces como zonas grises respecto a saber cómo funciona la araña y cómo se jala la información de los web masters, en este caso se les denomina a los dueños de los sitios web que les hemos llamado editores, pero finalmente son ellos los que podrían tener un motor de solución o un robot de exclusión para que el buscador no jale esa información y por eso.

Y yo que me cree en la red y aprendí, aquí hay varios de mis maestros en esta mesa. Todos los principios de protección de datos, todos los derechos arco y cómo se deben atender por un responsable de tratamiento, ahora que estoy de este lado pienso que por ejemplo, el buscador cuando dicen que decide sobre el tratamiento, realmente el

buscador lo que jala es todo tipo de información por ejemplo, sobre rocas ígneas, sobre situaciones geográficas, sobre datos históricos, sobre arte y cuestiones que no tienen información personal, ningún dato personal.

Y esa información se obtiene del web master, porque no está con un robot de exclusión, igual que un dato personal, o sea, que está en el cúmulo de las cosas que hay en internet y de esa manera el buscador es un espejo que sólo refleja lo que hay en los sitios, como dijo el abogado general en sus conclusiones, que después no retomó el Tribunal en su sentencia final.

Y por otro lado como les dije, queremos transmitirles que por ejemplo hablando ya en tema muy estricto técnico de protección de datos. Cuando se dice que el buscador o más bien, la sentencia traslada a internet los derechos de la electiva, creo que se utiliza el término buscador como sinónimo de internet, cuando no necesariamente es así.

De hecho si uno quisiera y se dice pues, que eso va impedir que se lesionen derechos de un titular, cuando se bajan los datos de un buscador y no necesariamente del sitio original. Pero eso no es así, porque si yo quisiera seguir lesionando los derechos de una persona y nada más se bajan del buscador, yo podría mandar un spam o subirlo a redes sociales o ponerlo en otro tipo de cuestiones en internet que sí podrían seguirlo lastimando. En ese sentido, no se garantiza de manera absoluta el derecho al olvido.

En Google queremos transmitir que queremos hacer las cosas bien, realmente respetamos la resolución pero sí nos encontramos inmersos en una delicada tarea de ponderar en cada caso la procedencia o no de eliminar la posibilidad de llegar a información de un individuo a través de la búsqueda por nombre y esto representa un nuevo y difícil desafío para nosotros, dado que caso por caso debemos analizar si prevalece el derecho a la protección de datos o el derecho a la información por existir un interés público.

Por ello y dado que Google realmente Google quiere entender a Europa, Google es una empresa americana, en Estados Unidos no se encuentra como en el debate de la gente, el querer bajar una

información del buscador y para poder entender bien se conformó un comité de expertos, los cuales están escuchando a docenas de profesionales en la materia a lo largo de todo el continente europeo.

Esto es para contar con elementos que nos puedan guiar en la toma de decisiones y vamos a estar muy atentos a lo que nos digan ellos, porque todos son expertos independientes, que tienen muchísima experiencia desde distintos prismas.

Pero quisiera nada más mostrarle o mostrarles cómo existen caso frontera y zonas grises que no resuelven la sentencia.

Por ejemplo, el caso de información de hace mucho tiempo de una figura pública muy relevante en la actualidad. Acuérdense que en el buscador vamos a encontrar información desde el inicio de la era humana, hasta la actualidad.

Y por ejemplo, nosotros tuvimos un presidente que en algún momento fue un alto ejecutivo de una compañía.

Si en su momento se hubiera podido ejercer el derecho al olvido en el buscador porque él ya tenía ser planes de ser político en el futuro, pudiera haberlo borrado, porque era el titular de los datos.

Pero los electores en el futuro no hubieran sabido esa información buena o mala, pero no se hubiera podido conocer.

Por ejemplo, información de personas que pudieran haber estado relacionadas en el pasado con una red de corrupción que se investiga en la actualidad.

En la actualidad se dice: ¿Por qué existe esta casa? Vamos a investigar.

Y esa información a lo mejor en su momento se pudo haber bajado.

Por ejemplo, que yo trabajo en una compañía constructora, quisiera mostrarles el sitio de Google donde pueden consultar información sobre cancelaciones de datos que ha hecho Google a partir de la sentencia.

Ustedes pueden ver ahí las solicitudes de privacidad que se han hecho en Europa y ustedes pueden ver el número de solicitudes, el total de URL´s que Google ha evaluado para su retirada, son más de medio millón y el número total de solicitudes que Google ha recibido son 167 mil 165.

Google lo puede hacer porque es una gran compañía, pero si existiera un buscador menor o con una actividad en otros rubros, que tiene pocos empleados, pero que manejan millones de usuarios, yo no sé cómo podrían atender a estas solicitudes.

Pero afortunadamente la compañía lo puede hacer y aquí tenemos ejemplos.

Esto es público, ustedes lo pueden ver, incluso las discusiones del comité de expertos y si ustedes dan clic van a ver ahí los casos en donde ha decido Google bajar o no bajar una compañía privada ponderando derechos.

Aquí tenemos un caso en Alemania, que quiero resaltar, en donde por ejemplo, una víctima de violación solicitó remover una liga, una nota periodística relativa a ese delito.

Google procedió a remover ese sitio de los resultados de la búsqueda por el nombre de la persona.

Otro ejemplo, una persona solicitó a Google remover las ligas, artículos que hacen referencia a su despido, en virtud de la comisión de delitos sexuales en el lugar del trabajo.

Google no removió estas ligas de los resultados de búsqueda.

Y así pueden ustedes verlos.

Desde el punto de vista rigurosamente técnico-jurídico, la sentencia, y esta ya es una opinión como experta en protección de datos, creo que desmembra la unicidad del derecho a la protección de datos tal como se concibió originalmente en la directiva, ya que crea una nueva figura y no por la vía de la regulación. De lo que podría interpretarse como

parcialmente responsable, sin que deba cumplir, por ejemplo, el buscador con el principio de información, calidad, licitud.

El buscador no podría corregir datos, porque no conocería la naturaleza del tratamiento, no de avisos de privacidad de todos los sitios que se suben. Los buscadores en tanto que intermediarios no otorgan todo este aviso de privacidad, etcétera.

Entonces es difícil sin conocer el aviso, conocer las finalidades y, por tanto, eliminar.

¿Cómo operaría, por ejemplo, el bloqueo? Eso es lo que yo aprendí en materia de protección de datos.

Antes de cancelar hay que bloquear.

¿Eso supondría, por ejemplo, consultar al web master original? En fin, y ya para terminar, porque me está quedando muy poquito tiempo. En este foro se ha debatido acerca de la naturaleza de un buscador como fuente de acceso público.

Quiero decirles que para México el internet es una fuente de acceso público, de acuerdo a nuestra Ley Federal de Protección de Datos en Posesión de los Particulares. Y eso está en el artículo siete, fracción I, del reglamento de la ley, que define a internet como una fuente de acceso público.

¿En ese sentido si un buscador se considera responsable para efectos de protección de datos requeriría el consentimiento para indexar los datos que obran en las páginas web en México? Diríamos que no, porque eso es una fuente de acceso público exceptuado el consentimiento.

¿Pero en otras latitudes que no consideran al internet como una fuente de acceso público sí tendrían que recabarlo? Pareciera absurdo pensar que así tuviera que ser dependiendo del país. En fin.

Para ir cerrando los buscadores sí juegan un papel preponderante en el trabajo de historiadores, periodistas, incluso de autoridades investigadoras de delitos, y también tienen un rol garantistas, ya que

gracias a los buscadores nos podemos enterar del mal manejo que se pueda dar a nuestra información en múltiples sitios, de modo que vamos a ejercer nuestros derechos ARCO.

Creo que cada región tiene el legítimo derecho a decidir qué publicita y qué no. en el caso de Canadá, por ejemplo, y Estados Unidos la información de ex convictos o abusadores sexuales, pues es de interés público saber dónde viven, en fin, hay muchísimas cuestiones que quisiera abordar, pero voy a ser muy respetuosa del tiempo de los demás para escuchar y estar muy atentos a lo que nos pueden aportar para poder cumplir de mejor manera con esta resolución.

Muchas gracias.

Óscar Guerra Ford: Muchas gracias, Lina. Gracias por acotarte al tiempo. Y qué bueno, se planteó en este encuentro escuchar las diversas posiciones que en muchas yo veo muchas áreas de confluencia y las otras hay que seguirlas trabajando, conocer la opinión, en este caso de las empresas de Google, y la Red Iberoamericana sabrá cómo, en su momento, procesa estas discusiones y toma las decisiones que considere más pertinentes.

Voy a dar a continuación el uso de la palabra al maestro el Filosofía del Derecho Noé Riande Juárez, quien es profesor del posgrado de la Facultad de Derecho de nuestra Universidad Nacional Autónoma de México, que hoy está de fiesta porque su Abogado General fue nombrado el Presidente de la Comisión Nacional de Derechos Humanos. Le deseamos mucho éxito. Perdón por el paréntesis.

Entre su experiencia se encuentra ser Subdirector de Educación en la línea de Estudios Sobre Justicia Fiscal y Administrativa del Tribunal Federal de Justicia Fiscal y Administrativa, y Presidente fundador de la Asociación Nacional de Investigadores en Informática Jurídica, Asociación Civil.

Y Noé, como decimos aquí, tienes hasta 10 minutos.

Noé Riande Juárez: Antes que nada muchísimas gracias. Gracias por esa invitación. Gracias al IFAI. Gracias a las autoridades del IFAI que

tuvieron confianza en mí, y obviamente a la Secretaría Permanente de la Red Iberoamericana.

Como escucharon soy abogado, soy filósofo del Derecho, pero me he dedicado desde siempre a la informática jurídica. Me dediqué originalmente a sistema de inteligencia artificial, y así fue como tuve la fortuna de conocer a muchos de los aquí presentes, hace muchos años; a don Erick, a Lina, a Ana Brian; Ana desde el ’89 trabajábamos en un desarrollo de inteligencia artificial para el Senado de la República.

Y en esta ocasión nos encontrábamos trabajando el tema de los sistemas cognitivos para ver de qué manera el conocimiento jurídico se podría trabajar, a partir de un análisis epistemológico de cómo es que se desarrolla el conocimiento jurídico.

Y fue así como llegamos al punto que vamos a tratar.

El tema que se nos presentó a tratar, obviamente contemplaba algunas otras cosas que las traté de manera muy rápida y que en esta ocasión las voy a obviar, precisamente por la falta de tiempo.

Las preocupaciones básicas en nuestra materia fueron desde el principio el flujo transfronterizo de datos personales, el email, el spam, las listas de exclusión que nunca funcionaron y sin fusionar, al menos en México, la situación de las cookies y el marketing que hacen insuficiente toda la advertencia previa, que ese es un tema sobre el cual me voy a centrar más adelante y del cual nada más aviso ahora que lo que es una de las preocupaciones básicas en nuestro ambiente.

Tenemos además el problema de las redes sociales, dado que ahí planteamos, no solamente datos personales, sino datos acerca de las acciones e interacciones que realizamos, dando oportunidad a que por efectos del análisis de esos datos, se provoquen incluso lesiones físicas o lesiones morales a la dignidad, a la economía, a través de diferentes métodos, como pudiera ser la ingeniería social, ciberacoso, la venganza pornográfica, la ingeniería de mercado orientada al cliente, que es un tema sobre el cual vamos a volver y bueno, aquí con las redes sociales, más que advertencias previas, lo que se requiere

son alianzas con los proveedores de redes sociales, para educar a la gente.

Y ese tema lo dejamos como una preocupación básica, otra preocupación básica la de Cloud Computing, que ya ha sido tratado abundantemente en la reunión del año pasado, en donde se dejó en claro que es necesario no solamente que se le obligue al responsable, a tratar, a establecer medidas de seguridad respecto del Cloud Computing, sino que además es necesario educar a la gente en torno a este fenómeno para poder realmente ofrecer seguridad en el manejo del Cloud Computing, y ahí hay una serie de especificaciones que se han señalado en el evento pasado, en el Congreso pasado.

Ahora, el problema al cual me quiero abocar o al cual me aboqué cuando hice esta presentación, fue el procesamiento de la información, porque el procesamiento de la información lo que hacemos cuando trabajamos en informática, y es exactamente lo que, como filósofo del derecho, estudio desde el punto de vista de la epistemología.

Bien, el procesamiento de la información que tiene varios aspectos, tales como valoración, clasificación, recapitulación, agregación, análisis e interpretación, me permite tener nuevas percepciones del conocimiento, no solamente.

Además la experiencia me permite llegar a nuevas soluciones, generar innovaciones, llegar a nuevas expectativas y concebir inclusive nuevos paradigmas, esta es la realidad con el procesamiento de la información hoy en día.

Esta realidad que es en la que nos encontramos ahora, implica una serie de actividades tales como aprendizaje, razonamiento, atención, memoria, resolución de problemas, toma de decisiones, procesamiento del lenguaje entre otros y podría yo seguir aumentando más y más elementos que forman parte de estos, procesos que son a final de cuentas conocidos como procesos cognitivos y esos procesos cognitivos son elementos que estamos realizando como usuarios o como empresarios que hacemos uso de las red o como usuarios de la red desde cualquier posición estamos procesando información y estamos llevando a cabo cualquiera de estas actividades.

Y me centro en esto, porque no solamente quisiera señalar y atacar a los problemas que vamos a ver más adelante, sino porque es realmente admirable que esto que hacemos cotidianamente se pueda reproducir por medio de sistemas inteligentes.

Los sistemas cognitivos son sistemas inteligentes que se logran concretar gracias a que ha habido estudios desde mediados del siglo pasado, en donde la psicología, la neurología, la epistemología, varias ciencias tradicionales y nuevas ciencias como la inteligencia artificial y algunas otras, las neurociencias, por ejemplo, han contribuido a dar los elementos para poder concretar este procesamiento de la información que hoy en día nos hace posible hacer evaluaciones tan sorprendentes como las que me permiten en un momento dado tener abierta una página de internet junto con otra persona, la otra persona tener también abierta la misma página, pero estar viendo diferentes cosas, porque la computadora nos está ofreciendo respuestas diferentes, porque nos ha analizado y nos ve como entes que tenemos gustos mínimamente diferentes. ¿Y por qué? Porque ha habido una evaluación de nuestras personas de nuestros hábitos.

Entonces, para poder hacer esto se necesita analizar a fondo qué es la cognición, esto que es lo que se dedica la ciencia cognitiva, en realidad nosotros hemos afrontado fundamentalmente tres aspectos de estos procesos cognitivos: La memoria, la percepción y la atención. Y que si lo vemos desde el punto de vista de la protección de los datos personales, la parte que tiene que ver con la memoria ya la tenemos de alguna manera sujeta, porque hemos controlado el almacenamiento y la recuperación de la información.

La parte que tiene que ver con la percepción también la tenemos controlada porque el procesamiento de la información lo tenemos bastante bien descrito respecto de cómo controlarlo a través de nuestros ordenamientos.

Pero la parte de la atención que es una parte en donde se dan fenómenos que tienen que ver con el big data, con el internet de las cosas, la atención nosotros la ubicamos como la focalización de la actividad cognitiva.

Esto es, cuando la computadora es capaz de reconocer que yo he centrado mi atención por más de tres segundos en un ícono y luego otro dentro de una página de internet, me está haciendo una valoración de en qué estoy focalizando mi atención.

Este aspecto todavía no está bien regulado y vamos a ver más adelante qué es lo que sucede en la gestión del conocimiento desde el punto de vista empresarial está entendida como una premisa, como una capacidad para realizar todas estas cosas que están aquí.

¿Por qué? Porque el conocimiento es una representación simbólica de lo real, se representa en un algoritmo y se trabaja con esa representación.

Me produce reducción de costos, me produce reducción de tiempos, mejora de calidad del producto, etcétera, pero esto lo hago gracias a que hemos desarrollado tecnologías de especialización de audiencias.

¿Les suena conocido tecnologías y especialización de audiencias?

Y esas tecnologías de especialización de audiencias que se apoyan en una gran cantidad de base de datos que son generadas de manera aleatoria. ¿A través de qué? A través de las cookies y a través de algunos otros elementos.

Les pongo un ejemplo de cómo IBM está presentando un metabuscador que hoy en día hace análisis más allá de los que hacían los metabuscadores que nada más buscaban en los buscadores.

Ahora hacen búsquedas en los buscadores y además hacen análisis y esto gracias a algo que se conoce como las “cookies de sincronización” no están contempladas en los análisis que se han hecho del Artículo 122, al apartado 2, del Artículo 122 de la Ley de las Sociedades de Servicios de la Información Española.

¿Por qué? Porque ahí clasifican las cookies nada más conforme al listado que vemos en la pantalla y vemos que se señalan todos estos intermitentes.

Pero la verdad es que no se dice cómo es que emplean las empresas de análisis y medición o las redes publicitarias o las mismas agencias de publicidad estas cookies de sincronización.

Esas cookies de sincronización permiten la entrada de otras personas, de otras empresas que no son precisamente quien contrató el servicio del anunciante y que hacen que se llegue, que se le abra la puerta a quienes no se les dio originalmente permiso para entrar y analizar la información.

Habría más que decir de estas cookies de sincronización. Es realmente una debilidad en la realidad normativa europea y ya no se diga en nuestro país donde apenas sí esperamos que en el futuro se contemplen una reglamentación del uso de las cookies por parte de… está vagamente señalado, pero habría que ampliarlo muchísimo más.

Pues con esto concluyo.

Muchísimas gracias.

Óscar Guerra Ford: Muchas gracias, maestro Noé, y la verdad sí lamentamos el corto tiempo que tenemos para todos los ponentes. Pero así son las cosas. Se quedará la presentación, y si es el caso del documento para que sean consultados por todos los interesados.

Voy a dar a continuación la palabra a nuestro invitado el doctor Frank de la Rue, quien como todos sabemos fue Relator Especial de la Naciones Unidas Sobre Promoción y Protección del Derecho a la Libertad de Opinión y la Expresión.

En el 2003 fue nombrado para recibir el Premio Nobel de la Paz, por su labor como defensor de los derechos humanos.

Es abogado y Director del Instituto Centroamericano de Estudios para la Democracia Social. Es miembro fundador y fue Director del Centro para la Acción Legal en Derechos Humanos. Se desempeñó como Comisionado Presidencial para los Derechos Humanos en Guatemala del 2004 al 2008, además de haber sido profesor en diferentes instituciones guatemaltecas y tiene en su haber participado en

muchísimos foros internacionales relacionados con los derechos humanos.

De verdad es un honor y agradecemos la visita en este Instituto por segunda ocasión del doctor Frank de la Rue.

Y está en uso de la palabra, Frank.

Frank de la Rue: Muchísimas gracias.

Yo quisiera agradecer profundamente al IFAI, a todas las comisionados y comisionados este gran honor y esta gran posibilidad de estar en este Encuentro Iberoamericano de Autoridades de Protección de Datos.

Con Catalina Botero, mi colega, que era relatora también del Sistema Interamericano. Seguimos muy de cerca el ejemplo de México, y particularmente los temas de acceso a la información pública, y hemos felicitado la experiencia de México de los pocos países que ha logrado institucionalizar profundamente el acceso a la información, y con la última reforma constitucional convertir al IFAI en un ente federal autónomo, que me parece a mí que es un paso realmente muy, muy significativo.

Deseamos lo mejor al IFAI, y además le ofrecemos toda nuestra colaboración desde las nuevas posiciones que nos tocarán jugar en derechos humanos.

Yo voy a ser muy breve, por razón del tiempo, pero sí quisiera hacer mención a algunos de los temas que yo levanté en el Consejo de Derechos Humanos de la ONU y en la Asamblea General, como parte de mis informes, de varios informes, pero todos vinculados al tema de privacidad y manejo de datos.

Lo primero, yo tuve los primeros dos informes sobre internet en el 2010 en el Consejo y en la Asamblea. Y lo que a mí me interesaba, y sigue siendo mi interés, es trasladar el enfoque de derechos humanos al internet y al entendimiento que tenemos del internet.

El internet, por supuesto, puede, el profesor nos lo hacía ver muy eruditamente ahorita, puede ser visto desde múltiples formas de vista. Puede ser visto desde el punto de vista filosófico, la epistemología del conocimiento, el manejo de la información y de datos, puede ser visto desde el punto de vista técnico, puede ser visto desde el punto de vista empresarial, puede ser visto desde el usuario, desde los pueblos, o desde los pueblos en lucha, como fue el caso de Egipto o el de Túnez.

Yo creo que desde múltiples visiones, y por eso se dice que el internet debe ser entendido en un diálogo multisectorial, y a mí lo que me interesaba era agregar la dimensión de derechos humanos. ¿Por qué? Porque además estamos frente a un fenómeno real, varios de ustedes lo han mencionado, que la legislación de nuestros países cambia de jurisdicción en jurisdicción, de distrito jurisdiccional.

Y no puede ser que en materia de derechos humanos y en derechos fundamentales como la libertad de expresión, o la privacidad, tengamos legislaciones que entren en contradicción.

Legislaciones distintas, sí, es un tema de soberanía por supuesto y cada país tiene la legislación que quiere, pero se entiende y esto es parte del consenso mundial, que toda la legislación redactada soberanamente, debe encajar con las normas internacionalmente reconocidas en convenios o en instrumentos internacionales, de derechos humanos y que no pueden entrar en contradicción.

Esto es el interés más importante.

La Presidenta Dilma Rousseff, de Brasil, usó este argumento, creó muy importantemente en su discurso ante la Asamblea en el año pasado, cuando dijo efectivamente el enfoque de derechos humanos es lo que nos va a permitir uniformar una visión común del uso del Internet, incluyendo el tema del acceso que fue mi siguiente informe, porque no dije que el acceso mismo era un derecho, pero sí dije que la libertad de expresión y ejercer la libertad de expresión, necesita de acceso y que todos los estados deberían de hacer un esfuerzo especial de garantizar acceso a los sectores más pobres, más rurales de sus respectivos países.

Todo mundo me advirtió que iba a haber una masiva protesta de los países, por estarme metiendo en temas económicos, ningún sólo país, ni un país levantó la voz en contra de este principio y creemos que es un principio y que sigue siendo válido; el internet no debe ser parte de la derecha digital o de la derecha académica, entre quienes saben manejar esas nuevas tecnologías, o quien tiene el poder económico o las posibilidades de hacerlo y los sectores más pobres de cada país, o entre Continentes y diferentes países.

El internet al contrario debe de ser el instrumento de acercamiento y el instrumento de desarrollo, de ejercicio del derecho al desarrollo común, por eso estamos insistiendo que el año entrante lo incluyen en las metas del milenio que está siendo discutido.

Rápidamente paso.

Yo hice un informe también, el año pasado en junio del Consejo, sobre privacidad y libertad de expresión.

Mi mandato no abarcaba privacidad, ahí sí como buen latinoamericano me aventuré a introducirme en un tema que no era mío realmente; pero cuál fue el argumento.

Primero, no hay un relator sobre privacidad, y segundo, lo que yo plantee es que quien ve libertad de expresión, tiene que hablar de privacidad, porque son dos derechos distintos, bien diferenciados y hay que entenderlo así, pero van de la mano.

Sin privacidad no puede haber libertad de expresión. ¿Por qué? El que nos estén violentando nuestros datos, nuestra información, nuestra comunicación o nuestras publicaciones o la prensa, o nuestros libros o nuestros escritos, esa violencia contra el contenido de nuestros mensajes, nuestro arte o cualquier forma de expresarse, implica un esfuerzo inhibitorio, intimidatorio de la expresión.

Entonces, que proteger la privacidad es esencial para proteger la libertad de expresión. Por eso es que van de la mano.

En segundo lugar plantee que efectivamente los estados pueden en momentos excepcionales, y esto tenía que ver con el monitoreo de

información de los estados por el tema de seguridad nacional, en momentos excepcionales, como lo era en el pasado con los teléfonos o retrotrayéndonos a un pasado todavía más lejano, con la correspondencia, si había indicios específicos de la comisión de un delito, o de un hecho que pudiera ocasionar un daño público grave, pero que tenía que haber un motivo específico, tenía que haber un interés público claro, y tenía que haber un procedimiento idealmente judicial, para poderlo hacer.

Y en segundo lugar, tenían que haber órganos de monitoreo y control de cómo se hacía esta intervención, porque el peligro que yo veía en el mundo de hoy y lo he dicho públicamente, he dado conferencias sobre esto, es que en aras de la seguridad y porque el terrorismo sí ha aumentado y hay más riesgo en el mundo, lo cual es cierto, tenemos un mundo más peligroso.

Entonces, se ha permitido que agencias de seguridad o de inteligencia por sí y ante sí tomen la decisión de a quién monitorean o cómo. O hay estados que van más lejos y le permiten a empresas privadas que sean las que decidan a quién monitorear, incluso en el caso de Corea del Sur había una comisión de estándares, porque para no hacer el monitoreo del estado, el estado le exigía a las empresas, a los servidores de internet que fueran ellos quienes lo hicieran, que me parecía que era incluso introducir un intermediario con lo cual se hacía más complejo.

Este informe sigue siendo discutido, Alemania y Brasil han estado planteando la necesidad de establecer un mecanismo en procedimientos especiales del Consejo de Derechos Humanos de la ONU, para el tema de privacidad.

Posteriormente en la Asamblea General del año pasado en octubre, en el 2013, presenté un tema distinto, pero también vinculado a acceso a la información pública y a veces a privacidad. Y era el derecho a la verdad.

El derecho a la verdad es un derecho muy de origen latinoamericano, trágicamente surge de la lucha que en América Latina seguimos para la búsqueda de nuestros desaparecidos.

En mi país Guatemala, en Argentina, en Chile se empezó esta terrible práctica desde la décadas de finales del 60's, inicios de los 70's y efectivamente esta búsqueda de los desaparecidos y las desaparecidas, implicó una demanda al estado de información, hasta el extremos de que movimientos permanecieron, las madres de la Plaza de Mayo, las abuelas, los familiares, FEDEFAM, familiares desaparecidos.

Y esto llevó a la Comisión Interamericana y después a la Corte Interamericana a establecer a establecer el que se llamó derecho a la verdad, que no es ni más ni menos que establecer la verdad de las violaciones a los derechos humanos, no es el enfoque filosófico de qué es la verdad, porque en esa sí tendríamos mucho que discutir, sino no era una cosa mucho más concreta: La verdad de cómo se violaron los derechos humanos, quién lo ordenó, quién lo hizo, si se procesó alguien, hubo justicia o no.

En Naciones Unidas se fue todavía un paso más allá, se empezó a discutir los principios contra la impunidad, el profesor Luis Joan, de Francia y más recientemente la actualización de los principios por *Dyan Olinker*, una profesora de Washington de la American University.

Y es interesante porque el principio cuarto si mal no recuerdo, es el que dice: Normalmente uno identifica la verdad con la justicia, o sea, la verdad es el primer paso para la justicia, lo cual es cierto. La verdad de las violaciones debe conducirnos a la justicia.

Pero se llegó a un punto más fino todavía, pero no debe olvidarse que la verdad por sí misma tiene mucho poder y esto es muy relevante para el manejo de datos, ojo, y para el manejo de lo que se quiere recordar o se quiere olvidar, porque la verdad dice: Tiene en sí misma también el poder de ser un instrumento para derrumbar el muro de la impunidad.

La Corte Interamericana lo ratificó en un caso en El Salvador con el caso de la masacre del Mozote, porque eran los familiares, la comunidad del Mozote pedía al estado salvadoreño la información sobre la masacre y el estado dijo: "No, porque los posibles procesados ya no se encuentran".

Y como no va a haber proceso penal, entonces no tenemos obligación de liberar la información, porque no hay ni fiscalía, ni nadie que nos la pueda pedir.

La Corte Interamericana les corrigió la plana y le dijo: “No va haber proceso penal y no va haber información en un juicio penal, pero eso no quitan –decían- no borra el derecho a conocer la verdad que tiene la Comunidad del Mozote.

Entonces, el conocer la verdad de los hechos es un derecho fundamental cuando se trata de violaciones a los derechos humanos.

Yo fui más lejos en mi informe, planteo y esto es muy relevante con lo que se está discutiendo en México en las leyes ahorita, estuve hoy con viejos amigos en el Senado, no tuve oportunidad de ir al cámara baja por tiempo, ¿pero cuáles son las regulaciones del estado?

Tanto en Argentina, como en Uruguay, en la Ley de Acceso a la Información sí establece claramente que la información relativa con violaciones de derechos humanos no puede tener ninguna excepción, ni de seguridad nacional, porque claro, sería muy fácil decir: se implica a un presidente o a un ex general o alguna persona que todavía es importante, entonces no se va a poder mencionar sus nombres o sus datos porque eso puede desestabilizar al país. Eso ya no es argumento.

Si hubo violaciones de derechos humanos nadie puede borrar ese hecho, ni las responsabilidades individualizadas de quienes lo cometieron.

Lo dejo ahí.

El siguiente tema, con mucha rapidez, fue el que hice en la Asamblea General, recién pasada dejé mi informe, era “Niñez y Libertad de Expresión”.

Ahí trato de muchas cosas, pero el tema de internet era básicamente que ha sido mencionado por varios de ustedes, de que la niñez debe gozar de los mismos derechos que todo adulto. O sea, no son adultos

pequeños con menos derechos y eso implica el acceso a internet y eso implica privacidad.

Pero al mismo tiempo la niñez merece protección. Entonces ahí sí tenemos un dilema, porque cómo protegemos a la niñez y al mismo tiempo le damos pleno acceso al internet y al ejercicio de su libertad de expresión.

Yo no creo que haya una dicotomía, yo no creo que libertad de expresión y protección están en contradicción. Ambos son necesarios para la niñez, pero sí debemos de resolver ese dilema complementariamente, padres de familia, comunidad y el estado mismo. ¿Cómo se prepara a la niñez, cómo se educa a la niñez, a los adolescentes y a los jóvenes a usar el internet positivamente?

Y termino con la resolución de España y la sentencia de la Corte Europea, que me ha interesado mucho, pero me preocupa y lo digo en dos palabras.

Yo creo primero que toda sentencia de Corte debe ser respetada.

Me parece que no podemos pensar que porque no estoy de acuerdo, no se cumpla, me parece que hay una sentencia de la Corte y debe ser cumplida. Ahí no hay vuelta de hoja.

Pero en segundo lugar, sí pienso que hay un dilema aquí para mí, que es un dilema de visión muy diferente entre Europa y América Latina y por eso lo digo en este Foro Iberoamericano, y es que en la medida en que América Latina nos movemos hacia la reconstrucción de la memoria histórica de nuestros pueblos y la reconstrucción del tejido social y la investigación de las atrocidades del pasado, de las violaciones de derechos humanos o la investigación de la corrupción que sigue siendo uno de los grandes cánceres de nuestro tiempo en la democracia.

En Europa salieron de esa etapa con las Segunda Guerra Mundial y hoy quieren moverse hacia no, mejor protejamos la privacidad de individuos que quieren olvidarse de lo que hicieron en el pasado.

Este es un dilema complejo, no lo vamos a resolver hoy aquí. Pero primero sí quisiera dejar claro que el derecho al olvido, como derecho no existe, es un nombre que alguien se inventó, a un nombre bonito le puso Derecho, pero no hay un derecho ni al olvido ni a ser olvidado.

De hecho yo oí un ponencia muy buena que se llamaba “El fin de lo efímero”, porque decía antes lo efímero eran las palabras porque se las llevaba el viento, y lo permanente era lo que escribían. Hoy irónicamente invertimos la lógica y escribimos como hablamos, y a veces no reflexionamos mucho en lo que ponemos en internet. Pero efectivamente eso hoy queda más grabado que lo que antes escribíamos en papel. Hoy ya no hay comunicación efímera.

Y esto tiene que ver con, lo que queremos es reconstruir historia, lo decía la Bibliotecaria General de Madrid, dijo: “La historia no es de héroes, guerreros y guerras, sino es de los pueblos y de todo mundo”.

Recientemente tuve la oportunidad de conocer al historiador Ginsburg, de Italia, que dice exactamente lo mismo: “La historia es del pueblo, y la hacen todos los ciudadanos comunes y corrientes de los pueblos”.

Entonces pensemos en términos de historia hasta dónde queremos borrar la historia.

Ojo que no me estoy refiriendo a la información usada maliciosamente para dañar la honra y la reputación. Eso, por supuesto, es una violación de la privacidad y debe ser borrada.

Entonces en conclusión el principio que yo planteo es lo que era privado en su momento, si se violentó debe hacerse privado borrando información. Pero lo que no era privado en un momento dado no tiene por qué convertirse en privado hoy. No hay razón.

Y el único caso medio límite es el caso penal, Europa tiene mucho esto de que después de haber cumplido una sentencia penal y reintegrarse a la sociedad y después de cierto número de años cada país tiene diferentes, se le borra el record judicial.

Si el hecho estuvo en la prensa no se le va a borrar los periódicos, pero sí se borra el record en el sistema de justicia.

Ahí, para mí, es un punto nebuloso que hacer a pesar de que lo delitos de extrema violencia o de acoso sexual me parece a mí que deberían de permanecer para la protección de las víctimas. Esa es un poco mi posición.

Creo que el olvido no es un derecho y que para empezar tendría que llamarle de otra manera. Muchísimas gracias por esta oportunidad.

Óscar Guerra Ford: Muchas gracias, Frank. Nos has dado muy rápido un pequeño resumen ejecutivo de las grandes actividades que has desarrollado como relator en tu trabajo, muy apreciado.

Y finalmente yo también cerraría con una frase de un historiador mexicano: “La historia es de los vencedores, pero también hay historia de los vencidos, y deberíamos de saber cómo los vencieron”.

Voy a dar la palabra ahora, se ha incorporado, como se han dado cuenta a la mesa a Danilo, que lo vamos a dejar que se distraiga un poquito del tráfico, y le vamos a dar mientras la palabra al maestro en Ciencias Políticas y Gobierno, Erick Iriarte, quien es miembro fundador de la Sociedad Peruana de Derecho Informático. Actualmente es socio principal de Iriarte y Asociados y Director Ejecutivo de Alfa Redy.

Se desempeñó como delegado por Perú para coordinar el grupo de trabajo Sobre le Marco Regulatorio de la Sociedad de la Información y de Internet, de la Plataforma eLAC.

Y fue coordinador de las metas sobre el marco regulatorio de la Sociedad de la Informática del Plan eLAC 2007-2010 y 2013.

Erick Iriarte Ahon: Creo que lo dejas ahí, porque si no.

Óscar Mauricio Guerra Ford: Si nos pides, porque es largo y eso que me hicieron un pequeño resumen.

Te lo agradezco, Erick y estás en uso de la palabra.

Erick Iriarte Ahon: Gracias, muy amable.

Es para mí un honor estar aquí, gracias a la Presidenta del IFAI por la invitación.

Normalmente mis presentaciones son bastante díscolas, por llamarlo menos y en este contexto ya Fernando me ganó en la mesa anterior en ser díscolo, pero también Claudio Magliona ayer y la presentación de Pablo Palazzi también fue bastante irruptiva, a su manera y todos han ido presentando textos bastantes irruptivos y presentaciones irruptivas.

La idea básica es, y además quiero expresar aquí un abierto reconocimiento al IFAI, es no solamente mirarnos el ombligo y dedicarnos a hablar dogmáticamente los mismos temas, sino comenzar a mirar qué más hay ahí, más allá del árbol que miramos, sino en el bosque en el cual estamos.

La protección de datos personales, sin duda es un derecho monobásico que todos defendemos. A mí me tocó ser parte del equipo que desarrolló la legislación en Perú, no soy parte de la autoridad, con quien discrepo en algunos puntos, pero sin duda, si alguien esperaba que hablara sobre mis discrepancias con la autoridad, éste no es el Foro, sino los foros nacionales donde corresponden.

Así que hablaré sobre este primer punto, que pido que coloquen el video.

(Proyección de video)

Trataré de hablar de algo, respecto a la legislación. Hablaré de algo.

A los que tienen Twitter, mí Twitter es @coyotegris, los invito a que me sigan, es un dato público, por llamarle de alguna manera. Pero para que les quede más claro y voy a ser absolutamente claro y creo que voy a violar todos mis principios de datos sensibles, soy mestizo, católico, heterosexual, pro unión civil, liberal, proliberal, prointernet libre, pero divorciado, apriísta, que es algo más o menos como ser del PRI.

¿Por cuál de ustedes esos me van a segregar hoy? Para eso creamos los datos personales, creamos para evitar abusos, para abusos de los

nazis, utilizando computadoras de alguna compañía en los 30's en los censos, lo creamos para evitar nuevos estados ficticios como 1984 donde todo está controlado, lo creamos para proteger a la gente.

Y esta protección que hicimos para todos nosotros es un derecho humano básico, está así en la Declaración Universal de Derechos Humanos.

Pero las tecnologías nos enfrentan a cosas interesantes como la deep Web, nos preocupamos porque los buscadores tengan información de nosotros. Los buscadores poco más, poco menos que reflejan el 5 por ciento del internet, 5 por ciento, 95 por ciento ocurre en lo que se llama la deep web, ¿quiénes han entrado a la deep web, levanten su mano, porque en teoría es para ilegales? Tú que haces levantando la mano.

Yo he entrado a la deep web y ustedes probablemente también sin darse cuenta. Alguien ha ido por el silk route, el camino de la seda, tráfico ilícito de armas, drogas, sexo, gente esclavos, la big data nos enfrenta a retos constantes de qué queremos hacer con los datos, quién los manipula y nos olvidamos que muchas veces la mayor manipulación de los datos viene del estado mismo, que es el que tiene más datos de nosotros.

El cloud computing pensado tanto como los datos que puedan manejarse en el cloud computing, pero también desde los estados, algunos estados prohíben si quiera que sus funcionarios tengan un correo Gmail o puedan colocar en servidores Gmail los correos institucionales, otros pueblos muy pequeños, diversos países del mundo colocan, porque es más barato utilizar un sistema Gmail de correo electrónico para gestionar sus dominios.

Tenemos los Rfid, las radiofrecuencias. Nos comentaban ayer que algunos bares en Barcelona para su zona VIP se colocan un chip como su fueran un perro. Entonces, van y se identifican, pasan por alguna zona y tienen algún pase especial para la zona VIP, yo no me pondría ningún chip, pero alguna gente supongo que quisiera ponerle algún chip a la novia, a la pareja, para saber dónde se encuentra.

Alguna gente dice: Bueno, si los problemas son los servidores y la legislación aquí, pongámoslo en la luna, ¿no? Total, pongámoslo en

un satélite, pongámoslo en Marte, ahora con transmisiones directas de alta velocidad pudiéramos colocar los servidores ahí, ¿cuál es la jurisdicción aplicable?

O mejor coloquémosla en la Antártida, en teoría la Antártida es una zona liberada, podemos colocarlo ahí y, por supuesto, los selfies, en un ratito más tomo el mío con ustedes.

Pero yo en este momento me voy a quejar abiertamente del relator Frank, porque o revisó mi Power Point antes o alguien le sopló mi presentación.

Tenemos claro que hay un derecho nuestro a poder modificar nuestra propia historia, pero también hay un derecho del colectivo de mantener la historia.

Hay cosas que queremos olvidar y de pronto la tecnología no lo borra. Lo más sencillo son las deudas, el caso europeo termina siendo un caso de una deuda que alguien pago.

Los spring breakes que vienen aquí, sobre todo a la costa mexicana, sus hechos de juventud hay algunas fotos que algunos ni quisieran ver publicadas y que colocaron en Facebook.

Las versiones preliminares de nosotros mismos, podemos discrepar de lo que uno era un poco más joven o de los textos que escribía, pero por ejemplo, en propiedad intelectual uno tiene el derecho retirar la obra o lo tenía, al menos en un principio, retirar la obra del mercado. En temas digitales no se puede.

Las sentencias cumplidas y la reinserción social, entre otras cosas, dicen que la sentencia cumplida tú ya no debes mantener tu récord nacional, porque ya cumpliste tu pena.

¿Y qué pasa con los indultados y qué pasa con los conmutados de pena?

Los cambios de identidad sexual, si ahora eres María y antes te llamabas Juan, ¿quieres que se siga sabiendo que eras juan, sobre todo si te vas a casar con Rodrigo o con lo que fuera, con el nombre

que quieras? O la rehabilitación de vicios. Alguna gente es alcohólica, otra gente le gusta el tabaco, otra gente tenía otros vicios y no quiere que se los recuerden y no quiere recordarlo asimismo.

Pero la sociedad también tiene un interés, el primero es el acceso a la información pública, que es el otro lado de la misma moneda.

Aquellos que piensen que el acceso a la información pública es dispar de la protección de datos personales, ese que no entienden ni uno, ni el otro, porque son dos derechos humanos básicos entrelazados y, sin duda, el IFAI tal como está configurado y la Gesic que también tiene las dos instituciones dentro del mismo esquema son los ejemplos claros de cómo llegar hasta este punto.

Europa avanza muchísimo en protección de datos y recién está comenzando en el tema de acceso a la información pública.

Para nosotros el tema de acceso a la información pública fue clave para la lucha contra la dictadura de Fijimori, yo fui uno de los estudiantes que entre el 97 y 98 salía en la televisión, en la prensa, a hablar en contra de la dictadura, amigos míos fueron muertos en la Cantuta, que fue un lugar donde mataron estudiantes. Aquí han matado a 43 estudiantes y no debe quedar impune ese tipo de cosas.

Porque la impunidad nos mancha como sociedad y alguna gente trata de hacer revisionismos históricos, algunos jugando a ser abogados, otros jugando a ser políticos.

Hay corrupción de funcionarios que tampoco tiene que ser borrado de la memoria y si cumplieron de su pena, que se cumpla la pena, pero los hechos no pueden ser simplemente borrados de la historia, porque ahí están las obras faraónicas de algunos presidentes de algunas regiones de América Latina.

Los archivos y la memoria son absolutamente claros para mantenerlos vigentes. Al mismo tiempo que en la democracia ateniense se creaba el derecho de autor, con Platón, al mismo tiempo. Pericles establecía la necesidad de mantener archivos históricos, permanentes y vigentes.

Los muertos, todos los muertos no se olvidan.

Los crímenes de lesa humanidad no pueden ni siquiera en el menor de los asomos tratar de ser borrados de internet.

El terrorismo. Y algo que nos olvidamos y es que América Latina ya trabajó sobre el tema del derecho al olvido. No le llamó derecho al olvido, se llamó “La Sentencia Ulloa”.

La Corte Americana de Derechos Humanos el 2 de julio del 2004 estableció que la Corte de Costa Rica había actuado incorrectamente al validar un fallo menor contra un periodista, contra su diario que un ex político, cuyo nombre es lo suficientemente complejo para que sea difícil de confundir, había este periodista hecho una nota sobre él de una denuncia que había tenido en Bélgica, como funcionario diplomático.

Él pidió que se retirara el diario, una rectificación, que se retirara de la versión digital del diario, pero que además se retirara del internet. Esto es el año 2004, los buscadores Google, hace un ratito Lina hablaba de que recién es del 2008, bueno, esto es posGoogle.

Pero además una de las cosas que pedía era que la resolución que sentenciaba al periodista fuera linkiada a la nota original, una cosa bastante absurda.

Saca de internet la página de la Nación Digital en lo relativo. Perfecto, ya estamos acabando, respecto al mencionado Tribunal apercibió a los señores Herrera Ulloa y Vargas. En caso de incumplimiento podría incurrir en delito de desobediencia si no borraban la noticia de internet, lo cual era ya en el año 2004 humanamente imposible.

Finalmente la Corte Interamericana estableció el punto 101.5, que dice que no se puede retirar porque evidentemente hay una necesidad, era un personaje público en función pública, y simplemente no se puede revisar y retirar las cosas de internet sin que esto implique un acto de revisionismo.

Hay una prohibición de censura previa, para proteger el honor de un funcionario público es absoluto y no encuentra justificación alguna en las excepciones dispuestas en el artículo 13 de la Comisión

Interamericana de Derechos Humanos. Eso es clave de entender, es nuestra forma de entender que las cosas no se deben borrar.

Entonces, América Latina ya tiene una posición sobre el Derecho al Olvido, y es no vamos a olvidar, y esto tiene que ver absolutamente claro. A esto se le llama relatividad del tiempo histórico, por la relatividad y el espacio tiempo histórico, por la relatividad del espacio tiempo histórico.

No podemos aplicar dos soluciones jurídicas, culturales, económicas, de realidades distintas en procesos culturales distintos.

Y evidentemente hay un debate, ¿es un debate real? No, lo que tiene que haber es una conciliación entre los intereses jurídicos tutelados en ambos derechos fundamentales con los avances de la tecnología. Los datos privados son siempre, en principio, pero hay informaciones de publicidad.

Dos más, y con esto acabo. La primera es la regla de Heredia para la anonimización de sentencias judiciales, trabajadas también con el IFAI, el profesor Carlos Gregorio que un gran trabajo que ha hecho en América Latina, y que tiene que ser utilizado para la anonimización de sentencias, resoluciones y todo lo que quisiéramos colgar en internet.

Y concluyo con dos ideas. La primera cuando un gobierno busca controlar a su población monitorea, controla, censura su internet, y necesitamos un internet libre, abierto, nuestro para todos, con irrestricto respeto de todos los derechos humanos como base de nuestra democracia.

Para concluir, a ustedes que son funcionarios públicos, que son autoridades más allá de que la sociedad civil, el sector privado podamos discrepar de ustedes, les tiremos piedritas de vez en cuando o les mandemos cartas o lo que fuera, les recuerdo una única cosa que fue lo que aprendí en mi escuela, con los hermanos de La Salle y de mi padre: “Quien no vive para servir no sirve para vivir”.

Muchas gracias.

Óscar Guerra Ford: No, pues gracias a alguien que nos dijo algo. No, de verdad Erick. De verdad muchas gracias, aparte de hacer pasar un rato ameno, creo que lo más importante, nos has hecho reflexionar sobre la ponderación del saber y la privacidad, que creo que es fundamental.

Bueno, ahora sí voy a dar la palabra, le damos la bienvenida y de verdad, qué bueno que pudiste llegar, Danilo.

El doctor Danilo Doneda, es Coordinador General de Estudios y Monitoreo del Mercado del Ministro de Justicia de Brasil.

Ha sido consultor en materia de protección de datos de la UNESCO; es profesor de la Fundación Tulio Vargas, y agradezco igual que los comisionados, el lunes y martes estuvimos ahí en la Fundación, en un evento donde se presentaron resultados de transparencia en Brasil, muy interesante, estuvimos muy a gusto.

Además ha sido y es investigador garante para la protección de datos personales, fue en Italia.

Bueno, Danilo, de verdad, bienvenido y estás en uso de la palabra y te digo la regla, son hasta por 10 minutos.

Danilo Doneda: Muchas gracias, Oscar.

Perdón por llegar tan tarde, pero ayer estuve en un avión por cuatro horas y después el vuelo fue cancelado, lo cual fue un milagro llegar aquí ahora.

El tema que preparé, en la zona de las nuevas tecnologías de la protección de datos.

Quería hacer una breve y muy sencilla reflexión, sobre cómo garantizar la aplicación y la efectividad de las leyes y las normas de protección de datos, nuestra realidad en particular en Brasil y América Latina.

Empezando un dato muy conocido, un dato muy hablado, el derecho siempre naturalmente está retrasado, en relación a la agenda social y eso no es novedad, no es un dato de la sociedad de información.

La norma jurídica tradicionalmente nace cuando hay estabilidad con la seguridad sobre un diagnóstico, una situación de un problema de un hecho que va a ser penalizado, que va a ser considerado ilícito.

Muchas veces no es necesario llegar a la norma jurídica, porque las normas sociales se pueden encargar de algunas situaciones.

Pero siempre que se habla mucho de nuevas leyes para la tecnología, esa cuestión me viene a la mente, me viene también el mensaje de Norberto Bobbio, que decía que los derechos nacen cuando son necesarios, cuando son útiles.

Muchas veces vemos situaciones en nuestra historia reciente, con protección de datos y derecho de liberar la información y que es realmente necesario que los derechos nuevos nazcan.

Y cuando se trata de tecnología, hay algunos motivos que…, esa ocasión, un poco más compleja, al menos para nuestros ojos.

Primero, la dinámica, la velocidad de la tecnología estupenda, mucho mayor que cualquier elemento de transformación social, consistente, natural que hubo en épocas anteriores.

La imprevisibilidad de los efectos de la tecnología también, es también el hecho de relajación de la técnica, es relajación diversa, de la lógica, de la eficiencia de la lógica económica, muchos factores, entre ellos la dificultad de escoger las normas, los principios que tienen la relajación de la técnica, que no es neutra, pero que muchas veces parece neutra, y tiene efectos; por eso muchas veces, más hablar de la previsibilidad posible.

Debemos ahí ver también la penetración de la tecnología en nuestras vidas, en nuestro cotidiano que hace que la situación de la ecuación de derecho y tecnología, no solamente complejo, pero también muy importante la evidencia de una normatización sobre muchos aspectos, se haga primeramente, sea imperiosa.

Cuando llegamos al tema de los datos personales estamos viendo un tema, una materia donde todos los problemas del derecho de tecnologías se hacen presentes y algunas dificultades mayores se hacen presentes también, porque la privacidad es un derecho más, la privacidad y algunos aspectos de la esfera privada de las personas no son cosas que se pueden trasgredir, son cosas que hacen parte de la persona, hacen parte de la personalidad y aquí ante todo procurar medios de cualquier medios posibles útiles para proteger la persona ante los riesgos de la tecnología y también equiparar con eso con necesidades de la vida moderna, de la comunicación, del derecho a la información y tantas otras.

El hecho que la protección de datos está tan allegada a la tecnología no es una conclusión reciente, en el artículo de 1890, el famoso Riche Privacy the Warren Brandeis, estaba muy claro aquí, los autores detectaron, diagnosticaron la tecnología de la época, la tecnología de la época, la fotografía, el periodismo de masa, las grabaciones de audio, como nuevos hechos que cambiaron la actuación y el poder informacional entre ciudadano y ciudadano-empresa.

La simetría de la información que generó todas las reglas que tenemos hoy de protección de datos, se empezó a diagnosticar por más de 125 años.

Todo eso lo digo porque tengo una impresión que para tratar de leyes, de reglas que tratan de protección de datos es imposible no tener, no formularlas juntamente con la cuestión de su enforcement.

Las reglas de protección de datos de ninguna manera pueden ser aisladas de quién las va aplicar, de cómo se va aplicar, eso es del enforcement.

Es muy interesante el dato que hoy en noviembre del 2014 de 101 leyes de protección de datos que rigen alrededor del mundo, 92 de esas leyes, eso es más 90 por ciento, son leyes que prevén la existencia de una autoridad de protección de datos en diversos formatos, en diversas formar, pero es muy raro en la protección de datos que se deje solamente al Poder Judicial o los jueces, al

magistrado, todas las decisiones regulatorias y la apreciación de hechos, de fallos que dice respecto a protección de datos.

¿Por qué? Muy probablemente es muy importante el hecho que las tecnologías juegan un papel muy importante en todo el proceso de tratamiento, de procesamiento de datos, lo que hace con que una autoridad técnicamente capacitada, sea fundamental para disminuir la simetría informacional técnica-jurídica y otros matices también entre ciudadano y aquellos que detienen los poderes centrales de procesamiento de datos.

Lo digo tanto al sector privado, tanto el estado y muchas situaciones. Y lo digo eso porque es esa situación que tenemos presente y de modo muy claro.

Hoy en Brasil cuando se discute un anteproyecto de ley sobre protección de datos personales, la cuestión de contar o no con autoridad es el centro del debate actual y hay una opinión generalizada de algunos sectores en Brasil de que en el país como tenemos un sistema de protección al consumidor muy bien posesionado dentro de todo el territorio, como tenemos un ministerio público actuante en materias de defensa de los derechos humanos, derechos colectivos, derechos difusos, tal vez se deba dejar a esas entidades, a esos órganos la acción de la protección de datos.

Pero la verdad y creo que la experiencia de muchos de ustedes es capaz de comprobar eso, de que tanto el ministerio público, como la protección al consumidor no es capaz de arreglar y fiscalizar todo en materia de protección de datos.

Sí algunos puntos específicos al vez puede ser o ya tener alguna regulación específica de protección de datos de consumidores.

Por ejemplo, en esta semana se decidió en Brasil, en una sentencia muy importante que los sistemas de estados de crédito son legales a la luz de la legislación brasileña y que esos sistemas pueden y deben ser arreglados en los órganos de defensa del consumidor.

Eso es algo muy importante y es un ejemplo de un tema específico en protección de datos, en el cual la protección al consumidor puede jugar un papel importante.

Pero para finalizar, voy a traer un ejemplo muy claro en que el sector de protección al consumidor en Brasil actuó en un tema muy específico y técnico de protección de datos, en el cual encontró muchos problemas para actuar efectivamente.

Fue el ejemplo de una empresa que hizo un contrato con la empresa de telecomunicaciones en Brasil y que hacía el monitoreo de la conexión al internet desde el proveedor de conexión. Eso es el monitoreo para fines de publicidad comercial que muchas veces el contenido de la web era hecho a nivel de proveedor de conexión.

En la forma que era muy poco transparente y visible y controlable por el usuario.

Eso fue un fallo que llegó, fue un fallo que inició en el 2010, pero hay que recordar que la ley que se aprobó fue en Brasil, el marco civil de internet que tiene varios puntos referentes a la protección de datos, tiene un artículo muy importante que dice que prohibido a los proveedores de conexión monitoreara, filtrar, bloquear, analizar el contenido de los paquetes de datos de internet.

Hoy tenemos una ley y tenemos también un fallo en la situación que llegó a la protección de los consumidores.

Pero mi cuestión ahora es ¿cómo técnicamente esos órganos, tanto el judicial, como los órganos de defensa del consumidor van a constatar que de hecho el proveedor hace eso?

La situación fue muy complicada, de la absoluta ausencia de un cuerpo técnico y de reglas claras, que pudiesen definir lo que era el monitoreo, lo que era una bifurcación de la comunicación en internet, eso es el proveedor de conexión que no estaba solamente proveyendo pero también utilizándose de la información del contenido.

Esos hechos que tenemos claramente como derechos que deben ser defendidos técnicamente son muy difíciles de analizar y muchas veces

son para el técnico pueden ser, y va a ser contestado por otro. No es una solución ideal para la mayor parte de los casos.

La solución que fue dada en Brasil fue por una vía transversa. Eso es, se consideró que lo que el proveedor de conexión hacía, no era el mismo que el proveedor, con razón decía a los consumidores.

Eso es, se utilizó una vía transversa para decir que el monitoreo que el filtraje de contenido no era posible porque no estaba en el contrato y también había algunas sospechas que aquí referiría el principio de terminar el internet.

Pero eso es algo que parece como una solución para un caso que no se puede trasladar a otro. Para terminar, lo que quería decirles que ahora cuando pensamos en Brasil y una nuevo ley de protección de datos y aquí en México y diversos otros países, que están en diversos niveles de aprobación y legislación y de actuación, legislación en el sentido nos parece cada vez más claro que sin una autoridad con cuerpo técnico y con contenido, con conceptos técnicos bien definidos para enfrentar nuevas situaciones de nuevas tecnologías hay siempre un peligro mayor de que las leyes de protección de datos de las autoridades den normatividad meramente formal, meramente cosmética cuando algunos hechos de vanguardia, de tratamiento de datos que son los que efectivamente más dañan a los consumidores, puede ser cuas invisibles, y que es imperceptible a los andares de la ley y de las autoridades.

Muchas gracias.

Óscar Guerra Ford: Muchas gracias, Danilo, y hoy aprendí mucho en la Getulio Vargas, ya en tres días aprendí portugués, te entendí perfectamente el portugués, portuño. No, muy bien.

Voy a dar la palabra a nuestro último panelista y no por ser el último es el menos importante, sino igual de importante que todos los que nos acompañan en esta mesa.

Él me ha pedido obviar la lectura de sus datos curriculares, ya se dieron en una mesa que él participó, lo cual te agradezco Jesús, para

poder ahorrar tiempo, dado que estamos ya pasados del tiempo en que teníamos que terminar.

Bienvenido y te doy la palabra.

Jesús Rubí Navarrete: Buenas tardes.

Esta sesión ha tenido en alguna medida un carácter de repetición del primer debate que hubo al inicio del encuentro sobre la sentencia del Tribunal de Justicia, y por tanto me veo en la obligación de prescindir de parte de mi intervención y volver aclarar algunos conceptos para tratar de despejar algunas inquietudes que se han manifestado.

Me remito a la detalladas y exhaustiva exposición que hizo el Director de la Agencia Española de Protección de Datos en aquel momento. Pero voy a precisar algunos aspectos de una manera muy sintética.

En primer lugar, como él explicó, no se trata, esa sentencia no trata del derecho al olvido en internet. Ni las resoluciones de la Agencia de Protección de Datos de las que trae causas esa sentencia hablan del derecho al olvido en internet. Aunque es una expresión que es muy coloquial, que ha sido muy difundida en los medios de comunicación, técnicamente las sentencias y las resoluciones se refieren a problemas relacionados con el ejercicio del derecho de cancelación y de oposición.

En segundo lugar la sentencia no interpreta una directiva que parece o que se sugiere que es una directiva obsoleta, porque cuando se aprobó no estaban desarrollar buena parte de estos servicios.

La sentencia desarrolla un derecho de la carta de derechos fundamentales de la Unión Europea, que es el derecho a la protección de datos personales.

Y es una sentencia con una enorme proyección de futuro en Internet, como ponen de manifiesto entre otros aspectos, las numerosísimas reacciones que está generando en este entorno.

En tercer lugar, la sentencia garantiza la prevalencia del interés público en la información que se mantenga en la red; sólo incide en

aquellos casos en que no existe, no concurre ese interés público en la información.

Es el reverso, como dijo el Director, de la libertad de información.

Además, la sentencia, lo que implica o lo que supone es que la información continua en la web de origen, no se altera de ninguna manera, y puede seguir siendo accesible a través de los motores de búsqueda en internet.

La única limitación que introduce, en el caso de que no haya una prevalencia del interés público, es que entre los parámetros de búsqueda, no deba utilizarse el que está relacionado con el nombre y los apellidos.

Por tanto, sigue a través de cualquier otro parámetro, sigue pudiendo accederse a esa información que continúa inalterada en Internet, a través de los buscadores.

Y por tanto, la sentencia o la ejecución de la sentencia, ni altera la verdad, ni va a impedir, ni muchísimo menos, la investigación de la verdad, en casos tan tremendos como los que se han expuesto aquí esta tarde.

Ni impide la investigación histórica, porque la información sigue estando accesible, ni lesiona el derecho a la libertad de información.

Y por tanto, una correcta aplicación de la sentencia, estoy convencido que no va a producir los riesgos a los que se ha hecho referencia en algunas intervenciones en esta Mesa.

Y en cuanto a la posición del responsable del servicio de búsqueda, hay que tener en cuenta que sí, la sentencia dice que no hay otra categoría distinta, se podrá discutir de referenda, si tiene que haber más o menos categorías.

Tiene la categoría de responsable de tratamiento, y la tiene no por nada, ni por una edición caprichosa, sino por las decisiones que adopta en relación a la reconexión de información, a la ordenación de

esa información, a la elaboración de unos índices y a la colocación de los resultados.

Y esas decisiones las toma el buscador y por tanto, es responsable, aunque en algunas de ellas, pues la información o las decisiones que toma, no alcancen el nivel de transparencia suficiente para poder pronunciarse sobre ellos.

Dicho esto, para dejar otra vez claro cuáles son los términos de la sentencia y que por tanto, buena parte de estos riesgos no existen, voy a intentar de una manera mucho más sintética hacer una referencia al tema de la presentación.

A grandes rasgos, van a tener la presentación, por lo cual pueden ver el detalle.

Estamos en sociedades con un elevado desarrollo tecnológico, en un mundo globalizado, hay un desarrollo constante de nuevas tecnologías, hay ahí una relación de ellas y estas tecnologías van a generar ventajas en el desarrollo de nuevos servicios públicos y privados, en servicios privados y con nuevos riesgos para la privacidad y por tanto, hay que abordar estos desafíos para la privacidad con una mayor eficacia.

Estas tecnologías, las últimas tecnologías por qué se caracterizan, porque el incremento es potencial del volumen de datos que se trata, por el abaratamiento de los costos de almacenamiento y tratamiento de la información, por el incremento de las posibilidades y de las capacidades de procesamiento de los datos y de protestar los datos y obtener resultados en tiempo real.

Por la variedad de los datos que se procesan que provienen de una gran diversidad de fuentes, redes sociales, correos electrónicos, dispositivos móviles. El abanico es extraordinariamente importante, porque se toman decisiones automatizadas sin intervención humana y, sobre todo, porque todo esto tiene un valor económico y, por tanto, se monetiza y se pone en el mercado.

Y esto entre los riesgos para la privacidad están, el desequilibrio entre las empresas y los consumidores que afecta al consentimiento, el

desvío de la finalidad, puesto que se tratan los datos para fines distintos de los que se recabaron, el que se traten datos excesivos y no los datos imprescindibles para esa finalidad, el que los datos puedan ser inexactos, porque no se verifique la calidad de los datos y a pesar de eso se obtengan conclusiones y consecuencias sobre datos que no son exactos, porque se pueden tratar datos sensibles como son los datos de salud, porque la información se conserva durante periodos de tiempo mucho más allá de los necesarios para la finalidad que legitimó su uso, porque no hay transparencia, no hay una información clara a los afectados de para qué se va tratar la información, en qué términos se va tratar la información, hay una pérdida de control por parte de las personas sobre el tratamiento de los datos y se pueden generar dificultades para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Y por otra parte, aunque no sea exactamente un tema de protección de datos, este tipo de tratamientos pueden dar lugar a un cierto determinismo respecto de la conducta de las personas que se infiere del volumen del tratamiento de estos datos y situaciones de discriminación.

Las autoridades de protección de datos han tratado esta cuestión en múltiples dictámenes que los tienen ahí a su disposición y en estos están los principios comunes, son que hay que seguir garantizando la protección de datos personales, hay que tener una legitimación para el tratamiento que puede ser el consentimiento u otras causas, el interés legítimo, siempre que prevalezca sobre los derechos de las personas y no cuando sucede al revés.

Muy importante que haya transparencia, una información clara y accesible, la muestra algunas ejemplos que tenemos de lo que es la transparencia en la información en servicios de internet, pues no es verdaderamente recomendable. Uno de los casos que hemos tenido en la Unión Europea ha sido el *ejetic* de transparencia en la información, derivada de la unificación de la política de privacidad de Google.

El que se informe sobre finalidades específicamente y sobre finalidades genéricas que puedan permitir un tratamiento absolutamente abierto de los datos personales.

El que esté la información sobre el ejercicio efectivo de los derechos, que pueda incluir adicionalmente la posibilidad de obtener información sobre los perfiles que se hacen de las personas.

El poder obtener información sobre los propios procesos informáticos en aquellos casos en que se realicen decisiones automatizadas. En que se verifique la información para que responda al principio de calidad y al de minimización, es decir, que se utilice la imprescindible y durante el periodo de tiempo imprescindible que las finalidades sean determinadas y explícitas y que los periodos de conservación como he dicho, sean menores, sean mínimos y por tanto, se cancelen cuando sean innecesarios.

Y para hacer frente a estas nuevas situaciones, hay que desarrollar nuevas herramientas, herramientas predictivas, no me voy a referir a ello, ya lo ha hecho Ana Brian, la privacidad desde el diseño, la protección de datos por defecto que garantiza la minimización del uso de los datos y de los periodos de conservación, un aspecto muy importante que Ana Brian ha citado y que quería desarrollar brevemente, las evaluaciones de impacto en la protección de datos que deben realizarse cuando los tratamientos presentan riegos específicos para los derechos y libertades y respecto de los cuales la Agencia Española de Protección de Datos ha hecho, ha editado recientemente una guía donde pueden encontrar todo este tipo de soluciones, un análisis del tipo de riesgos del sistema, que es un análisis dinámico, no en una foto fija en el momento inicial del diseño de los servicios, sino que debe de continuar durante el proceso de desarrollo de esos servicios.

En la guía se hace una referencia a que los criterios que se recogen son flexibles, para que se puedan adaptar a distintos modelos de negocio y hay una relación de situaciones en las que sería recomendable realizar ese análisis y algunas medidas sobre cómo gestionar esos riesgos la tienen a su disposición en la web de la agencia.

Por tanto, nuevas herramientas, que como ha señalado Ana Brian, desde el origen del tratamiento de los datos acompañan a ese

tratamiento para que sea conforme con la normativa de protección de datos.

Y también en relación con estos tratamientos, otra alternativa que se plantea es la disociación, la no limitación de los datos.

Y hay que tener en cuenta en este sentido dos cosas, que la anonimización puede afectar a los datos de personas identificadas o identificables, pero que también hay normas que reconocen derechos a los usuarios, a los usuarios de internet, como es la Directiva 2002-58 de la Unión Europea, con independencia de que se trate de sus datos personales o no.

Y por tanto, en estos casos la disociación no será una solución para legitimar el tratamiento de los datos, porque los usuarios, aunque no sean identificables tienen derecho.

Pero la anonimización, no cabe duda, de que es una técnica que va a permitir hacer compatible, hacer compatible si se hace correctamente, hacer compatible el desarrollo de estos servicios con las normas de protección de datos.

Este dictamen que cito es un dictamen del grupo del Artículo 29 que reúne a las autoridades de Protección de Datos sobre la valoración y las técnicas de anonimización.

Y lo que me importa destacar del dictamen, es que la anonimización en sí misma es un tratamiento de datos.

Es decir, antes de anonimizar se tienen los datos personales. Y este tratamiento de los datos personales está sujeto a las garantías de la normativa de protección de datos.

Y por lo tanto, cuando se realice la anonimización, ese tratamiento anaonimizado debe ser compatible con las finalidades originales y se remite a otro dictamen del año 2013 en el que se señala cual es la compatibilidad con las finalidades.

También el dictamen hacía referencia a que puede haber, a que hay una legitimación para llevar a cabo estos procesos de asociación

basada en un equilibrio entre el interés legítimo del responsable que quiere realizar la anonimización y los datos y los derechos del interesado, pero con un aspecto muy importante que es en el que quiero llamar la atención.

Que hay que tener en cuenta que si se produce una disociación irreversible se pueden lesionar derechos de las personas, porque se impediría el ejercicio del derecho de acceso o de rectificación o de cancelación no, pero sí de acceso o de rectificación o de oposición, porque no se sabría o podría no saberse de qué son los datos de estas personas.

Y esto en algunos tratamientos masivos es muy importante, por ejemplo, en la investigación biomédica.

Si uno da una muestra biológica para obtener un resultado favorable de una investigación en la que se utilice esa información genética y después se disocian los datos, tiene que mantener sin una garantía de trazabilidad para que los resultados se puedan utilizar también en beneficio de esa persona.

¿Cómo se puede conseguir la neomilitación?
Hay un gran debate sobre si la anonimización a través de la tecnología es imposible, pero creemos que es posible complementar las medidas técnicas de anonimización con medidas organizativas, siempre que tengan eficacia jurídica.

En ese dictamen se hace referencia, en el que se analiza el *open data* y la reutilización, pues se incluyen algunas de las previsiones que permitirían completar la tecnología en la anonimización.

Muchas gracias.

Óscar Guerra Ford: Muchas gracias, Jesús, por también en el tiempo hacer la exposición. Una disculpa a los panelistas. Sé que diez minutos no es suficiente, pero el tiempo es el peor enemigo de estos eventos y de estos paneles, y lo peor, no he dado la peor noticia. Es que no vamos a poder abrir una ronda de respuestas y comentarios finales, habíamos acordado tres minutos, pero ustedes pueden ver el tiempo, son casi las ocho de la noche. Teníamos planteado iniciar la

clausura a las siete y media. Si doy tres minutos a cada uno nos estamos media hora cuando menos más, y puedo tener altas represalias por los organizadores.

Por lo cual les pido, y los comprometo a que las preguntas que le han hecho llegar y las que les harán llegar, puedan enviar las respuestas a los correos, que espero hayan puesto los que han solicitado esta información, pues para poder, cuando menos, de alguna forma dar respuesta porque hay derecho a la información y hay derecho a recibir respuestas por parte de las gentes.

Entonces también les pido una disculpa a los que hicieron estas preguntas, pero así son las cosas.

No habiendo más asunto qué tratar y no teniendo más tiempo damos por terminada esta mesa y los invitamos a que pasemos a la clausura.

Gracias.

--oo0oo--