Presentación de los trabajos de los subgrupos de la Red Iberoamericana de Protección de Datos Personales

Mesa 9

Moderador: José Luis Piñar Mañas. Presidente de la Red Iberoamericana de Protección de Datos Personales.

Voy a ser sumamente breve, tan sólo quería explicar el contexto en el que se mueven los cuatro documentos de la Red Iberoamericana de Protección de Datos, que en este momento vamos a presentar.

Como ya tuve ocasión de señalar ayer, la Red Iberoamericana de Protección de Datos se constituye en el año 2003, en particular en el Encuentro Iberoamericano que tuvo lugar en la ciudad de la Antigua, en Guatemala.

En mayo del año 2004 se celebra el Encuentro de Cartagena de Indias, en el que se aprueba una declaración, junto con unas conclusiones de entre las que en este momento me interesa resaltar la que se refiere al desarrollo de la Red Iberoamericana de Protección de Datos.

Como ayer señalé, habíamos recibido la muy grata noticia de que en la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, celebrada en Santa Cruz de la Sierra, Bolivia, en noviembre de 2003 se había hecho una expresa referencia a los trabajos de la Red Iberoamericana de Protección de Datos impulsándola, potenciándola y apoyándola en su labor.

Habíamos, por tanto, asumido un compromiso que no se podía quedar en simples declaraciones, aún siendo éstas sumamente importantes. No se podía quedar tampoco en simples buenas intenciones, sino que tenía que materializarse en algo concreto, en una aportación concreta a la comunidad iberoamericana en el ámbito de la protección de datos personales.

Y esto es lo que en estos momentos queremos presentar ante todos ustedes. Uno de los resultados del trabajo intenso, creo que serio, bien hecho de cuatro subgrupos de trabajo constituidos precisamente en la Cumbre de Cartagena de Indias en el ámbito de la Red Iberoamericana de Protección de Datos. Estos cuatro subgrupos han elaborado, como digo, cuatro documentos, sendos documentos que vamos a hacer públicos, que se van a colgar en las páginas Web de las instituciones que constituyen la Red Iberoamericana, que van a ser objeto de una publicación.

Tales documentos son los siguientes:

Primero: Acceso a la Información y Protección de Datos Personales.

Segundo: Viabilidad de creación de Autoridades de Control de Protección de Datos en Iberoamérica.

Tercero: Gobierno Electrónico y Telecomunicaciones en el ámbito o su incidencia en la protección de datos.

Cuarto: Estrategia de la Red Iberoamericana de Protección de Datos.

Estos documentos han sido elaborados y la labor de coordinación de relatoría se encargó a uno de los miembros de la Red Iberoamericana.

En particular la coordinadora relatora del documento sobre Acceso a la Información y Protección de Datos Personales, se acordó que fuese el IFAI, evidentemente, y dentro del IFAI ha sido la maestra Lina Ornelas la que se ha encargado de la coordinación de los trabajos.

Va ser ella quien nos va a hacer la presentación de dicho documento y a continuación se presentará también el resto de los documentos.

Ponente: Lina Ornelas. Directora General de Clasificación y Datos Personales del IFAI.

En lo particular yo coordine el grupo, a nombre del IFAI, de Acceso a la Información y Protección de Datos Personales.

Y a grosso modo les voy a explicar cuáles fueron los hallazgos del grupo respecto de este tema.

Básicamente lo que se hizo fue introducirlo planteando, por una parte, la necesidad de que las sociedades democráticas cuenten con un derecho de acceso a la información con autoridades o mecanismos institucionales que lo garanticen y se desarrollan los principios del acceso a la información como que el derecho debe ser gratuito, que toda persona puede pedirlo sin explicar las razones, cómo deben ser los procedimientos, etc.

Por otra parte, en una sociedad democrática debe existir la protección de los datos personales, desarrollando también sus principios, como lo son el de calidad, proporcionalidad, seguridad en los datos, etc.

Y luego para entrar ya a la parte medular que plantea el documento de trabajo, que sería que existe en ocasiones tensiones entre ambos derechos, pero lo que propone el grupo en este documento es más bien plantear que no se está frente a una tensión, sino más bien frente a un equilibrio de derechos, porque todos los derechos no son absolutos en sí mismos y encuentran limitaciones.

Entonces, esta necesidad de conciliar, por una parte, el derecho a conocer y el derecho de las personas a acceder a información, también tiene que equilibrarse evidentemente con el derecho a la privacidad. En este juego todos los involucrados deben respetar reglas claras y entonces se habló de, por ejemplo, una prueba del interés público o del equilibro, en casos de tensión.

Tanto el derecho como el acceso a la información pública como el de protección de datos personales, podrían someterse a una especie de prueba de equilibrio por parte de las autoridades competentes.

Y en estos casos tenemos que ponderar y valorar varias cuestiones. Por una parte, en el acceso a la información encontramos excepciones y una de esas excepciones son las relativas a las causales que la misma ley establece, por razones de Estado, que son del interés general, como lo sería información relativa a la seguridad nacional, etc.

Pero también las leyes de acceso traen excepciones por información confidencial que

es de los particulares. Entonces, en cuanto a modelar una especie de prueba de equilibrio, nosotros encontramos que podrían aplicarse algunos principios.

Por ejemplo, que deberían tomarse en cuenta los siguientes elementos. Una autoridad debe resolver el conflicto, de manera fundada y motivada. El fundamento debe encontrarse previsto de manera expresa en alguna ley. Luego, deben establecerse condiciones de procedimiento tales que aseguren la debida garantía de audiencia a los titulares de los derechos en conflicto, y finalmente deberá realizar esto a petición de parte.

Es muy importante que ustedes después conozcan el contenido detallado del documento. Dado que no tenemos el tiempo suficiente no podríamos ahondar más en los casos prácticos que se modelan en el mismo.

Pero les puedo adelantar que se establecieron algunos supuestos concretos de este equilibrio de derechos. Por ejemplo, en el caso de información ambiental en donde la información sobre la calidad del medio ambiente se considera de interés público y cuando hubiera una solicitud de acceso a la información, por ejemplo, acerca de una persona que con su actividad empresarial contamina un río o la atmósfera, etcétera. Si el conocimiento de ciertos datos personales llegara a constituir en un elemento esencial a través del cual se puedan determinar las causas que motivaron ese daño al ecosistema, entonces podría justificarse la publicidad de los mismos en razón de acciones que pudieran adoptarse para revertirlo o impedir su avance. A través de una prueba de interés público, necesariamente tendría que darse a conocer los datos personales del que está contaminando y el consentimiento para difundirlos por parte de su titular se encontraría disminuido.

Otro caso es el de la información acerca de funcionarios gubernamentales. Cuidadosamente se analizó que las personas tienen el derecho a conocer datos personales de los servidores públicos, pero éstos tienen que estar establecidos en normas y de no ser así entonces también tendríamos que aplicar una prueba del equilibrio para determinar si la información que se está solicitando está estrictamente ligada a la función pública del mismo funcionario o del mismo servidor.

Y ahí planteamos algunos ejemplos novedosos que se han dado, por ejemplo, sobre solicitudes de acceso al currículum vitae de los funcionarios o sobre las fotografías en donde se piden sistemas de datos personales en donde ha habido un avance jurisprudencial y administrativo y también de los tribunales, en algunos casos.

En este caso la prueba del equilibrio se enfocaría en si existen excepcionas a favor de la publicidad de dichos supuestos en leyes respectivas y si con la divulgación de los datos personales se puede vincular o conocer el correcto desempeño de las responsabilidades o tareas asignadas a un funcionario público. También si dichos datos son considerados como información propia del individuo o no, en fin.

Otro caso muy importante, y ya casi termino, es el de los expedientes médicos, donde ustedes saben que los datos relativos a la salud son datos personales, los estados de salud físicos o mentales. Estos están contenidos a su vez en archivos clínicos y se parte del supuesto de que el paciente goza de una prerrogativa para conocer la información sobre su estado de salud físico o mental.

Sin embargo en algunas regulaciones se precisa que el acceso a los datos de carácter médico únicamente puede obtenerse a través de un profesional de la medicina o bien que el paciente sólo tiene derecho a un resumen del expediente médico, el cual no contiene, por ejemplo, notas evolutivas.

Aquí también se somete a una prueba para tomar e cuenta que son datos objetivos relativos a información clínica del paciente y que podría ser una información subjetiva. En fin, lo interesante del documento es que se enfoca al

ámbito iberoamericano, pero también en las conclusiones observamos que existen diferentes modelos que guardan grandes diferencias entre los sistemas de garantía y tutela del derecho de acceso a la información, así como de protección de datos personales.

Estas diferencias sustantivas afectan de manera real y efectiva su protección, poniéndose de manifiesto la necesidad de contar no sólo con instrumentos legales específicos en cada materia que comprendan los mecanismos institucionales y procedimentales adecuados, pudiéndose apuntar a la conveniencia de contar con autoridades de control independientes.

Observamos distintas deficiencias en cuanto a la delimitación de conceptos tales como intimidad, información pública y confidencialidad que deberían ser definidos con mayor precisión posible a fin de limitar el grado de discrecionalidad de los órganos decisorios ante las solicitudes de acceso a la información pública.

De todo lo analizado, finalmente, se desprende que las leyes de acceso a la información pública existentes responden a ciertos criterios: el derecho de toda persona física o moral para tener acceso a documentos administrativos generados u obtenidos por el Estado sin acreditar su personalidad jurídica; la determinación de los sujetos obligados por la ley que no corresponde en Iberoamérica a criterios uniformes, no todas las leyes de acceso tienen los mismos sujetos obligados.

Y un procedimiento expedito y un recurso de revisión ante las negativas que pueda ejercer el ciudadano ante uno órgano eficaz y, por su parte las leyes de protección de datos personales deberían responder a un modelo que tuviera una serie de principios y derechos reconocidos a favor del titular de los datos personales y parte de principios básicos que ya hemos mencionado.

En los casos de tensión es importante contar con un procedimiento para dirimir y lograr el equilibrio del que hablamos porque se considera que entre el derecho a la información y el derecho a la protección de datos personales no existe a priori una verdadera colisión, pugna o conflicto, por lo que no debiera dirigirse la atención a una realidad filosófica previa, sino más bien es necesario que las autoridades administrativas competentes o bien aquellas con facultades jurisdiccionales o coasijurisdiccionales en la materia resuelvan de manera armónica y *ad casum* la cuestión.

Moderador: José Luis Piñar Mañas. Presidente de la Red Iberoamericana de Protección de Datos Personales.

A continuación tiene la palabra María José Blanco, para presentar como coordinadora relatora del documento el referido a viabilidad de creación de autoridades de control de protección de datos en Iberoamérica.

Ponente: María José Blanco. Subdirectora General de Registro de Protección de Datos Personales de la Agencia Española de Protección de Datos.

El documento de viabilidad de creación de autoridades de control en el entorno Latinoamericano refleja el resultado del grupo de trabajo creado en la declaración de Cartagena de Indias, en el Encuentro Iberoamericano del pasado año.

Y parte de la consideración de que consolidar el derecho fundamental a la protección de datos exige una contrapartida y es que existan mecanismos rápidos y efectivos de garantía y defensa de los ciudadanos en relación con el derecho a la protección de datos, ya sea de los poderes públicos o de los particulares.

Partiendo de la conveniencia y necesidad de disponer de estas autoridades de control, el documento recoge algunas recomendaciones dirigidas a los países de la Comunidad Iberoamericana en la que se describe un modelo marco de autoridad con amplios poderes de control que sería el modelo óptimo de creación de una autoridad de control y modelos

alternativos que puedan cumplir estas mismas funciones, pero con una estructura, competencias y organización diferentes, lo suficientemente flexible para que se pueda adaptar a cado Estado en función de sus peculiaridades jurídicas y sociales.

En el grupo de trabajo los participantes y los miembros de la Red somos conscientes de las posibles dificultades económicas y sociales que podría dificultar la creación de una autoridad. Y por ello propone el documento unas reflexiones para facilitar la creación de órganos de protección de datos que permitan garantizar este derecho.

En el documento, en el grupo de trabajo se realizó un análisis general de la situación en la que se pone de manifiesto que los flujos de datos transfronterizos son necesarios para el desarrollo comercial y social de los países iberoamericanos, que es necesario este flujo de datos transfronterizos tanto entre empresas establecidas en diferentes países de la comunidad, como entre las administraciones nacionales con fines de colaboración.

Se establece, por tanto, necesario impulsar la ración de medidas que garanticen un nivel de protección de datos adecuado y homogéneo en todos los países de la región, para eliminar esas barreras que en estos momentos podrían estar impidiendo el desarrollo de este flujo transfronterizo de datos.

Teniendo en cuenta que hay importantes diferencias en el nivel de protección de datos entre los países iberoamericanos y los países de la Unión Europea, ahí es donde se central el grupo de trabajo para intentar buscar alternativas a esta situación.

Si queremos que los países de la Comunidad Iberoamericana garanticen un nivel de protección adecuado respecto a la Unión Europea, según la Comisión Europea la autoridad de control es un elemento esencial en la protección de los datos personales.

En el documento se reflejan los distintos modelos de autoridad de control de protección de datos que se centran básicamente en el modelo europeo, creados según las previsiones del Convenio 108 del Consejo de Europa, de 1981, que luego recoge la Directiva 95 46.

Y las otras características de esta autoridad que preveía ya el Convenio 108 y la Directiva 95 46, que es el modelo que se transpone en el modelo español, las características de esta autoridad es una autoridad independiente, es el requisito, quizá, más importante, debe estar presidida por un director.

En el caso de la Agencia Española de Protección de Datos elegido entre los miembros de un consejo consultivo, con un mandato de cuatro años, sus decisiones sólo pueden ser revocadas por la Audiencia Nacional; actúa con transparencia en su actividad. Tiene la obligación de presentar una memoria anual en el Parlamento todos los años. La autoridad de control debe contar con poderes de supervisión para poder realizar investigaciones, inspecciones y, en su caso, imponer sanciones, garantiza la publicidad de los tratamientos de datos personales a través de un registro de protección de datos.

Facilita a los ciudadanos la tutela de sus derechos y resuelve las denuncias de vulneración de la Ley de Protección de Datos, y en el caso de la Agencia Española su presupuesto anual esta se financiado por los presupuestos generales del Estado y mediante otros sistemas de autofinanciación.

Se hace también un estudio de la situación latinoamericana, en la que el ejemplo de autoridades de control es la Dirección Nacional de Protección de Datos de la República Argentina, que se crea con un sistema de organización muy similar al que establece la directiva de protección de datos, y que en base a esto consigue la decisión de adecuación de la Comisión Europea, decisión por la que se considera la República Argentina como un país que ofrece un nivel de protección de datos

adecuado. Lo que favorece este flujo de información, de transferencias internacionales de datos.

El Grupo de Viabilidad establece unas reflexiones sobre una ponderación para elegir un modelo de protección de datos, un modelo de autoridad de control de protección de datos y en base a estos criterios realiza unas conclusiones en las que se ratifica en el documento que las autoridades de control cumplen un rol fundamental en la protección efectiva de los datos personales. Y propone como modelo de referencia el modelo europeo de autoridad de control que se describe en el documento.

No obstante, de acuerdo con las circunstancias de cada Estado, circunstancias económicas, sociales, los proyectos ideales de creación de estas autoridades pueden ir precedidos de soluciones alternativas y complementarias no excluyentes entre sí, y ofrece una serie de soluciones provisionales. La primera alternativa es utilizar la estructura administrativa, constitucional y judicial ya existente, y las funciones esenciales que debe reunir la autoridad de control. El grupo plantea que puedan ser asumidas por órganos administrativos, constitucionales o judiciales ya existentes, siempre con la condición de que mantengan su independencia en la toma de decisiones sobre protección de datos.

Otra alternativa sería crear órganos y mecanismos complementarios de protección en el ámbito público. El documento hace unas consideraciones de aquellos Estados en donde se va a implementar políticas de gobierno electrónico y modernización del Estado, se podría tener en cuenta las implicaciones de estas políticas en el ámbito de la protección de datos, y se propone que cuando un Estado vaya a adoptar estas políticas, se sopese la posibilidad de crear supervisores o encargados de protección de datos en este ámbito.

También se plantea como una posible solución, alternativa, la reestructuración de órganos administrativos y asistentes, creando nuevas unidades que no supongan incremento del gasto público, pero que sí permitan una racionalidad de los bienes materiales y personales, para garantizar este derecho fundamental que ha sido asumido en la *Declaración de Santa Cruz de la Sierra*.

Y por último, ya como última alternativa, en el caso de que no sea posible promover ninguna de las anteriores, promover una mayor colaboración del sector privado; favorecer el funcionamiento de expertos u oficiales de protección de datos, como medio eficaz de alcanzar mayores niveles de cumplimento e incentivar la autorregulación por los propios agentes interesados, por ejemplo, a través de códigos de conducta.

Moderador: José Luis Piñar Mañas. Presidente de la Red Iberoamericana de Protección de Datos Personales.

Y a continuación tiene la palabra la doctora María Alejandra Sepúlveda, Coordinadora Relatora del Documento sobre Gobierno Electrónico y Telecomunicaciones.

Ponente: María Alejandra Sepúlveda. Ministerio de la Secretaría General de la Presidencia del Gobierno de Chile.

Realmente junto a Jesús Rubí, Ana Viang, a Alfredo Chirino y con la colaboración de Fernando Argüello, hemos hecho un trabajo realmente muy coordinado, a pesar de que cada uno está en su propio país, que se deriva y se desprende del compartir visiones, del compartir anhelos, inquietudes, en torno a lo que significa el desarrollo de las tecnologías de la información y las comunicaciones y la consiguiente protección de datos.

Qué duda que vivimos en un tiempo nuevo, en un mundo en que las maneras de comunicarnos, de trabajar, de constituir nuestras comunidades, de constituir nuestras organizaciones, cambia de una manera muy rápida y muchas veces difícil de seguir y de asimilar adecuadamente.

Se contraen los conceptos de espacio y de tiempo y la forma en que lo vivimos; caen las fronteras, y es así como todos nosotros asistimos a este proceso de globalización, pero lo vivimos de manera distinta, dependiendo de nuestro desarrollo económico, del tipo de inserción internacional que tengamos, de la madurez de nuestras instituciones, de la cultura de nuestras comunidades.

Es por ello que nos sentimos nosotros muy convocados dentro de este mundo nuevo, para preocuparnos del desarrollo armónico de la tecnología y de la protección de los datos, ya que sabemos que incide directamente en el desarrollo competitivo de nuestros países y en la generación de un mayor bienestar social para nuestras comunidades.

Definición de gobierno electrónico. Nosotros entendemos el gobierno electrónico como el uso de las tecnologías de la información y de las comunicaciones que hacen los órganos del Estado, con el objeto de mejorar la atención y los servicios prestados a los ciudadanos, la eficiencia y la eficacia de la gestión de lo organismos públicos y, a la vez, fortalecer la transparencia y la participación de los ciudadanos.

De este concepto de gobierno electrónico se desprenden los ámbitos en que éste se expresa, que es en atención al ciudadano. En este ámbito se busca el establecimiento, por medio de la utilización de la tecnología, de nuevas formas de relación entre el Estado, el ciudadano, el inversionista y el empresario, que permitan realizar una gestión más eficaz, más eficiente y con independencia del lugar físico.

El buen gobierno se expresa en la utilización de las nuevas tecnologías, con el objeto de poner nuevas formas y procedimientos internos de los servicios que permitan el intercambio de información, compartir recursos y mejorar la gestión operativa de los mismos.

Y en el desarrollo de la democracia es cómo abrimos, a través de las tecnologías de la información, nuevos canales de comunicación que promuevan la participación del ciudadano.

Es importante en este punto hacer presente que el desarrollo del gobierno electrónico tiene como sentido un proyecto estratégico; es decir, la incorporación de las tecnologías por sí solas no bastan. Es necesario un proyecto estratégico y que se tenga claro cuáles son los aspectos jurídicos y tecnológicos que están asociados a ese proyecto, como también los culturales y de capacitación de los de los distintos funcionarios públicos.

En nuestro grupo de trabajo abordamos y vimos todo lo relativo a protección de datos, de lo cual se ha hablado en este Encuentro largamente, del recurso de la Hábeas data, los temas de privacidad, de seguridad de redes, seguridad de instalaciones, seguridad de comunicaciones, seguridad de los documentos electrónicos, normas estándares, todo lo relativo al acceso, la brecha digital y su inclusión, lo relacionado con la institucionalidad, que es necesaria tener para desarrollar en buena forma al gobierno electrónico, los temas vinculados a la firma digital y muy fundamentalmente todo lo relacionado con educación y con capacitación, tanto del ciudadano como de los funcionarios públicos y, lo concerniente al tema de la neutralidad tecnológica.

Ámbito de las telecomunicaciones. Aquí desprendemos de la **Declaración de Cartagena de Indias** que advierte sobre el riesgo en el tratamiento de los datos personales en el sector de las telecomunicaciones y se propone la necesidad de establecer garantías.

¿A qué se refieren estas garantías? A los datos de tráfico, al tratamiento de los datos de localización, a la prestación de servicios de valor agregado, a la introducción de facturas desglosadas, a servicios avanzados de telefonía, a guías de abonados a servicios de comunicación electrónica y a garantías tecnológicas. Estos son los aspectos fundamentales a los que se refiere el tema vinculado a las telecomunicaciones.

Vamos al tercer tema. El Spam. Consecuencias del Spam que se analizaron en el grupo de trabajo.

En primer término atenta contra la intimidad del ciudadano, viola el derecho de la protección de datos personales, hay un abuso del sistema de comunicaciones a nivel global, se crean problemas de seguridad, hay recursos de Internet utilizados con malos fines, hay problemas de confiabilidad en la Red que inhibe al ciudadano para realmente realizar aquellos trámites que sí le van a aportar beneficios, genera perjuicios económicos en la Red y tiene costos generales para la economía global.

De ahí la necesidad de definir políticas y estrategias tanto nacionales como internacionales que nos permitan hacernos cargo de este tema y de todas sus derivaciones que sería muy largo detallar.

Finalmente, tenemos múltiples desafíos desde el acceso hasta la inter operabilidad y tenemos mucho camino por recorrer.

Pero lo que sí queremos señalarles es que en el Red estamos comprometidos a avanzar en esta materia, a profundizarla porque tenemos claridad de que el desarrollo del gobierno electrónico y la protección de los datos personales contribuye al desarrollo económico sustentable en nuestros países, a la generación de mayor bienestar social para nuestras comunidades, especialmente para aquellos que están aún marginados y rezagados del progreso.

Moderador: José Luis Piñar Mañas. Presidente de la Red Iberoamericana de Protección de Datos Personales.

A continuación tiene la palabra el doctor Álvaro Canales para exponernos como relator y coordinador el documento: *Estrategia de la Red Iberoamericana de Protección de Datos*.

Ponente: Álvaro Canales. Subdirector General de Inspección de la Agencia Española de Protección de Datos Personales.

Creo que va a haber un antes y va haber un después del IV Encuentro Iberoamericano o de la Red Iberoamericana de Protección de Datos Personales.

Hablando para todos y no solamente para los miembros de la Red, como es obvio, en el auditorio que nos reúne hoy aquí, se dan ustedes cuenta de que el tema de la protección de datos de carácter personal es un tema dinámico; las tecnologías de la información y de las telecomunicaciones día a día nos van facultando, nos van posibilitando un tratamiento más eficiente y más ágil de nuestros datos personales.

Y estos avances son muy significativos y muy a valorar, pero creo que la protección de datos de carácter personal tiene como derecho fundamental que es un ámbito que trasciende a todos los ciudadanos, es un ámbito universal y es un ámbito integral.

Ninguno de los que estamos aquí ahora nos podemos ver sustraídos al tema del derecho fundamental, porque como ciudadanos, como clientes, como proveedores, en nuestra vida diaria se están tratando datos de carácter personal por parte de responsables públicos y empresas privadas y de ese tratamiento de los datos personales no se infieren resultados neutrales, resultados que no nos afecten, resultados que aunque no lo percibamos en un primer momento no puedan causarnos trastornos a nuestra vida, a nuestra intimidad, a

nuestro desarrollo de la vida tal y como nosotros hemos querido configurarla, en un ambiente individual, en un ambiente familiar, en un ambiente social de nuestra dimensión como ciudadanos y como personas.

Les quiero manifestar que el documento estratégico es un documento que prevé que la organización de la Red Iberoamericana es una organización que está abierta a todos los sectores.

En este Encuentro de México, por primera vez en este nacimiento ya se vislumbra que ya no es un pequeño bebé que da los primeros pasos, sino que ya es un, yo me atrevería a decir un adolescente, un mozuelo, una chica, un chico, que ya empieza a tener una problemática y una presencia en muchos sectores y, por tanto, creemos en este documento estratégico que deben ustedes saber que todos los sectores pueden estar representados en la Red Iberoamericana, si bien es cierto que con diferente presencia, en función de que los representantes que participen en la Red sean representantes de instituciones nacionales, sean representantes de instituciones privadas, universidades o simplemente sean personas físicas, particulares que tengan una inquietud y que quieran estar al tanto del conocimiento de trabajos y de actividades que tiene la propia Red Iberoamericana de Protección de Datos.

Y en este sentido abierto de la Red, el papel que ocupa es un papel muy académico, muy universitario, porque manifiesta el documento estratégico tres grandes preocupaciones: Una preocupación de surtir de información a todos aquellos que pretenden participar de la Red o que quieren consultar documentos de la Red, servir también de un asesoramiento técnico y específico para el tema de protección de datos y sirve como un foro de debate, porque ni todas las sociedades tienen un mismo nacimiento y una misma configuración a la protección de datos, al honor, a la intimidad, en fin, cada Constitución y cada sociedad es diferente y, por tanto, este Foro de la Red Iberoamericana es un foro muy enriquecedor en el cual nadie parte en una postura preeminente respecto de nadie, cualquiera puede proponer, porque legítimamente nadie se le puede negar su propio modelo y su propia actuación y su propia conformación de cómo quiere y hasta dónde quiere llegar en materia de protección de datos.

Siempre teniendo en cuenta los principios y garantías que disciplinan comúnmente el respeto al ciudadano y la consideración de su propia voluntad en el tratamiento de los datos que son propiedad del propio ciudadano.

Los nuevos retos que tiene la red en el documento estratégico se manifiestan muy rápidamente, de acuerdo con lo que les he venido relatando en dos aspectos: Uno importantísimo es la divulgación de la cultura de la protección de datos de carácter personal.

No sé si ustedes recuerdan y yo me permito poner este ejemplo en materia de consumo: no hace muchos años, todos los ciudadanos cuando nos hablaban de los posibles derechos, los posibles arbitrajes, las posibles sanciones, las posibles reconvenciones entre un fabricante y el ciudadano, entre un distribuir, entre un producto, entre un servicio, entre un producto financiero y el ciudadano, no lo veíamos del todo, aunque todos o la mayoría apreciábamos que iba a ser un avance significativo en lo social y en las sociedades democráticas desarrolladas.

Pues, bien, en la protección de datos la Red Iberoamericana aporta esta inquietud y entiende que es la promulgación y la difusión de la cultura de protección de datos es fundamental para esas sociedades democráticas. Y en este sentido, se crea en el documento estratégico un grupo de impulso normativo y de armonización de la legislación en materia de protección de datos.

Para finalizar, la Red cree que el documento estratégico lo recoge, que la Red Iberoamericana tenga una página Web propia dentro de Internet, actualmente debido a estos dos primeros años,

la Red Iberoamericana viene ubicando sus contenidos, sus foros, sus informaciones, sus estados de situación en los países en un apartado específico que aparece en la «*home*» de la página Web de la Agencia Española de Protección de Datos.

Creo que la mayoría de edad de este proyecto requiere, y así lo ha visto y lo ha recogido el documento estratégico que la Red Iberoamericana tenga su propia página Web y tenga su propia identidad y su propia dinámica de funcionamiento y de independencia respecto de la Agencia Española que ha venido, por decisión de la propia Red, asumiendo la función de Presidencia y Secretaría Permanente de la propia Red Iberoamericana.

Sin más, agradeciéndoles en nombre de la Red a este maravilloso país que nos haya acogido tan calurosamente, doy sinceramente las gracias.