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

Versión estenográfica de la Sesión 5: "Modelos institucionales para la protección de datos personales: Aprendizajes, retos y oportunidades", 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: Vamos a iniciar con esta Mesa Número 5: Modelos Institucionales para la Protección de Datos Personales, Aprendizaje, Retos y Oportunidades.

Originalmente esta Mesa iba a ser moderada por el Comisionado Francisco Javier Acuña Llamas, quien en este momento se encuentra en la Sesión del Pleno del Instituto Federal de Acceso a la Información y Protección de Datos.

El Comisionado se disculpa con ustedes, porque tiene que presentar ante el Pleno algunos recursos de revisión que hoy serán votados.

En su lugar, modera esta Mesa, el licenciado Jonathan Mendoza Iserte, Director General de Verificación del Instituto Federal de Acceso a la Información y Protección de Datos, a quien le cedemos el uso de la voz.

Jonathan Mendoza Iserte: Muy buenos días. Bienvenidos a esta Sesión Quinta, denominada Modelos Institucionales para la Protección de Datos, Aprendizajes, Retos y Oportunidades.

Damos la bienvenida a nuestros ponentes, el doctor Felipe Rotondo Tornaría, la maestra María de Lourdes Zamudio Salinas, el maestro Pablo Palazzi y el maestro Patricio Vallespín López.

Sin más preámbulo, ellos son los expertos, le vamos a dar el uso de la voz al doctor Felipe Rotondo Tornaría.

Hago una breve síntesis de su larga experiencia curricular.

El doctor Felipe Rotondo Tornaría, es profesor de la Universidad de la República y de la Universidad de Montevideo y Codirector del Anuario de Derecho Administrativo.

Es doctor en derecho y ciencias sociales, y doctor en diplomacia por la Universidad de la República.

Tiene diplomado en Dirección de Administración Pública en el Instituto Nacional de Administración Pública de España.

También es Presidente de la Unidad Reguladora y de Control de Datos Personales de Uruguay.

Por favor, doctor, la más cordial bienvenida para usted.

Felipe Rotondo Tornaría: Muchas gracias.

Buenos días. En primer lugar, deseo agradecer al IFAI y a la Red Iberoamericana la posibilidad de estar aquí con ustedes, y voy a referirme al tema de este panel, los modelos.

Estrictamente cuando uno está en estas actividades tiene uno la suerte de hablar luego de varios paneles, porque he aprendido cosas y han sido dichas muy buenas e importantes consideraciones sobre el tema que también me corresponde tratar, porque si ustedes se fijan el objetivo de este panel se refiere esencialmente al modelo, a la arquitectura posible de diseño institucional de las unidades reguladoras en materia tanto de protección de datos como de acceso a la información pública.

Y como hace un rato muy bien decía Isabel Davara y también Jacobo, quizá no está bien hablar de lo que yo empiezo hacer, o sea, en la primera transparencia sé que no lo gaste todavía.

Hice un esquema justamente del modelo europeo y del modelo norteamericano y se digo muy bien antes y realmente estaremos en el mismo caso.

De todas maneras a qué refiere, modelo en cuanto al régimen jurídico en materia de protección de datos y a la efectividad, a los mecanismos de efectividad que corresponden a ese régimen.

El modelo europeo como se caracteriza básicamente, por un régimen de protección de datos en el cual esto es considerado un derecho fundamental, el derecho al debido tratamiento de los datos personales, tienen una normativa general sin perjuicio de las sectoriales y esa normativa general tiene una radical esencia en principios que son justamente las bases esenciales, la estructura, el centro del sistema, incluido el eje del consentimiento.

También la exigencia de una autoridad específica independiente de control y entre otros aspectos, el principio de continuidad al cual también hizo referencia Nelson Remolina en el panel anterior, en cuanto a las transferencias internacionales, si existe el nivel adecuado de protección entre los países o los organismos internacionales correspondientes. La autorregulación es admitida pero como complementaria de la *hetereoregulación* legal.

Si hablamos del modelo norteamericano o estadunidense con la salvedad de que también recibió muy bien y que apoyo de Jacobo en el panel anterior, se dio una determinada visión sobre el control, sobre la información personal, pero vinculado esencialmente a la no intromisión gubernamental en la esfera personal, en la privacidad.

He visto esencialmente un derecho del consumidor vinculado a la libertad de comercio. La normativa es sectorial en materia financiera, de menores, de salud, etcétera.

La esencia dada la regulación y en materia de transferencias el tema de puerto de seguro al cual iba hacer alusión, pero me remito íntegramente a lo que refirió también en el panel anterior Jesús Rubí.

Podemos hablar luego de un modelo latinoamericano, esencialmente diría que en algunos aspectos sí, pero que no. ¿Por qué? Porque es concebido como un derecho fundamental reconocido por la Constitución expresa o implícitamente.

En el caso de Uruguay, por ejemplo, hay una norma que refiere a los derechos inherentes a la personería humana y allí está y así lo explicitado la región de ley al cual voy a referirme después.

La garantía del Habeas Data propio como lo llamamos, que es una garantía jurisdiccional sumaria, efectiva y específica que tiene constitucionalmente su primera aparición, digamos, en la época referida a protección de datos en la Constitución Brasileña de 1988.

La tendencia hacia el modelo europeo, tendencia no significa copia y a su vez con distintos matices a la directiva 95, a la legislación española, al Convenio 108, etcétera.

La incidencia de la Red Iberoamericana en cuyo Décimo Segundo Encuentro estamos y voy a referirme a algunos aspectos que importan en relación al Uruguay, por ejemplo, en el Sexto Encuentro la Red refirió el Convenio 108 como un referente, como algo que realmente lo es, como una normativa abierta, de vocación universal, también a la autorregulación en la Declaración de Cartagena de 2004. Obviamente, como dije antes ya, complementaria a la exigencia de estándares internacionales.

Ahora, hay diferencias entre los países latinoamericanos, algunas de ellas están mencionadas allí, pero hay más.

Por ejemplo, en cuanto a algunos países tienen legislación general, otros no la tienen y es sectorial, a eso refirió muy bien Nelson Remolina e incluso en su transparencia, al ámbito subjetivo.

¿Quién es el titular del dato? En el caso uruguayo lo voy a referir luego, es por supuesto, la persona física de determinado o determinable, pero se extiende lo pertinente a personas jurídicas. Hay otros países como Nicaragua, etcétera que también lo tienen, pero no es en general así.

Luego respecto a quienes son los titulares de las bases de datos, si es del sector público estatal o no estatal o del privado.

Al diseño anterior a la existencia o no de autoridades o de órganos garantes y cuál es su diseño institucional, sus competencias, a los aspectos vinculados a las transferencias internacionales.

Y luego también, y ustedes lo tienen allí en último lugar en esta transparencia, la ausencia de una regulación interamericana específica. Tema que es relevante y no fácil como fue tratado en el panel de ayer vinculado a la EOA, si pensamos en esa integración en la cual en la OEA está como parte también Estados Unidos de Norteamérica.

Porque creo que de otra manera, si fuera un nivel con esa inclusión tal vez podríamos llegar a un convenio internacional, aunque no es una tarea fácil.

Si paso a referirme al Uruguay, porque tenemos que dar señales de modelos y del modelo que yo puedo hablar más seriamente es el uruguayo.

Quiero señalar primero que Uruguay es un país unitario, es un país federal como México, de modo que no tenemos el problema de… o como Argentina, de manera que no tenemos el problema de distribución de competencias que acá se plantea obviamente.

También la pequeñez territorial de nuestro país y nosotros tenemos alrededor de tres millones y medio de habitantes. Ustedes imagínense que somos casi un barrio de México, Distrito Federal.

De todas maneras es lo digo con orgullo humano, pero las realidades hay que reconocerlas.

De todas maneras Uruguay está bastante avanzado desde el punto de vista de la conectividad.

Fíjense que hay datos del 2013, hay un 70.2 por ciento de hogares urbanos, la mayoría de la población uruguaya es urbana, más del 70 por ciento con acceso a computadoras, un 25.8 por ciento de la población urbana usa teléfonos inteligentes, un 26 por ciento de usuarios de internet se conecta en movimiento, un 22.1 por ciento de

personas de más de seis años usaron una tableta en los últimos tres meses.

No quiero cansarlos con datos, pero digo ya que es pequeño territorialmente, etcétera, por lo menos compensar en otro aspecto desde el punto de vista de una apertura a los medios tecnológicos. Que se ha hecho campaña en ese sentido al cual me voy a referir luego.

En la transparencia que ustedes tienen allí es una abreviación de lo que surge de la normativa vigente.

En el Uruguay se aprobó en agosto del 2008 una Ley de Protección de Datos. Había una ley del 2004 solamente para el sector comercial, esta es una normativa general. Y es a tres meses anterior a la Ley de Acceso a la Información Pública que es de octubre del mismo año, y como voy a referirme a las dos es que hago esta mención.

Y segunda mención que quiero hacer, que fue aprobado, digamos, estando el partido de gobierno actual, pero votaron absolutamente todos los partidos, o sea, no hubo ninguna oposición parlamentaria ni un voto.

O sea, que es la sociedad uruguaya la que está de acuerdo con este régimen jurídico, y no es un tema de gobierno en turno.

Esta ley del 2008 parte de la base como figura tiene una regulación general, se le reconoce como un derecho fundamental, prevén la acción judicial de *habeas data* en forma sumal y específica, hay un amparo general que requiere legitimidad manifiesta, acá no, simplemente que no se haya atendido como corresponde los derechos ARCO o en el tiempo debido o no se haya justificado que no se lo atienda.

Se incluyen los datos de todo tipo en cualquier soporte de personas determinadas o determinables. Se extiende en lo pertinente a personas jurídicas, abarca bases públicas y privadas; públicas, estatales y no estatales.

El ámbito objetivo es totalmente amplio respecto a todas las formas de tratamiento, tiene los principios que son, como la palabra lo dice los principios, la base del sistema jurídico. Juridicidad que incluye el registro de base, veracidad, etcétera.

Se prevé que si el titular con respecto al consentimiento que si se le requiere y el titular del dato no lo da en 10 días hábiles se considera negativo, en este caso a favor del titular del dato, se considera que no otorga seguridad, etcétera.

Respecto a las transferencias internacionales con países u organismos internacionales que proporcionen nivel adecuado de protección. Se ha adherido en ese sentido al régimen europeo.

Con respecto a los temas de consentimiento, daría para más, en cuanto que evidentemente no es lo mismo en el caso de datos sensibles que tiene que ser, incluso, escrito, expreso y escrito. En nuestra normativa se habla de dato, perdón, de consentimiento expreso.

Planteo esto porque es un tema en cuanto a lo del consentimiento tácito inequívoco que me gustaría tratar, pero no es el tema que corresponde o que me corresponde.

Con respecto a la ley de acceso, que ya les dije que es de octubre del mismo año de 2008, es un derecho humano frente a todo organismo público estatal o no estatal.

El silencio del organismo en 20 días hábiles acá, al contrario es que se otorga el acceso, porque es en realidad el principio de publicidad la transparencia, la divisibilidad, si hay una parte del documento que no pueda precisamente accederse, gratuidad, tanto el acceso como en protección de datos los derechos se ejercen gratuitamente, informalismo en favor del administrado, etcétera.

Se prevé también una acción judicial sumaria de acceso, hay obligaciones de transparencia activa, en México también existen, no voy a entrar en ello.

Las excepciones que son excepciones restrictivamente, por lo tanto interpretadas, son información secreta que tiene que estar solamente determinada por Ley, información reservada que el organismo lo puede determinar y tiene un tiempo, en máximo 15 años, y así puse algo que es una ley que modificó en diciembre del año pasado.

Se clasifica al generarse, obtenerse o modificarse la información en base a la prueba del daño. Eso es claro.

Justamente lo que hoy se hablaba también por Isabel, etcétera, respecto a cuál es el interés público, que ese está en juego, respecto a ese punto.

Y que por excepción, absolutamente por excepción, se puede clasificar de reservada al solicitarse un acceso.

Eso dio lugar a bastantes discusiones, salió en una Reforma del año 2013, y debe de darse cuenta a la unidad de acceso que puede no estar de acuerdo con esa decisión.

El último punto que ahí aparece, es la confidencialidad, y lo que quiero enmarcar es que es confidencial, de acuerdo a esta Ley de Acceso, todo el dato personal que requiera consentimiento informado. Esa sería entre las dos leyes.

También se establece, lo tendría que haber dicho antes cuando hablé de reservada, que puede ser declarada, digo puede, porque eso depende del organismo, aquella información que pueda poner en riesgo la vida, la dignidad humana, la seguridad o salud de una persona, o también se agregó en el 2013, afectar el libre desenvolvimiento, asesoramiento por parte del organismo que se trate en el proceso de formación de su voluntad orgánica.

Con respecto a todo esto, lo incluimos como dimensiones de la gobernanza electrónica. Y esto tiene que ver incluso por dónde están ubicadas las unidades de que estoy hablando.

No voy a referirme, me encantaría, a lo que es la gobernanza. Ahora el Diccionario de la Real Academia incluye el sentido de la palabra ordenanza, a mí me gusta mucho la definición, de manera que me

remitiría a ella, y obviamente que es un gobierno y una administración de aplicación basadas en Internet y en otras tecnologías, portales de gobierno, etcétera.

Es clave decir la participación, la simplificación de los procesos del Estado y la normativa regulatoria; son los cimientos que es lo que me importa marcarles.

Fíjense entonces en la importancia de estas leyes, estamos considerando la Ley de Acceso en la Información Pública, la Ley de Protección de Datos, la de firma digital, que es un poco posterior, pero al mismo tiempo, y la del uso debido del poder público, o sea, una Ley Anticorrupción para llamarla como usualmente se les llama.

Esto está involucrado también a la existencia y regulación de procedimientos administrativos electrónicos, a normativa sobre la interoperabilidad, que entiendo que se está cumpliendo adecuadamente, en base a principios.

Esto tiene que ver con la institucionalidad, que es un poco el tema que me corresponde.

Fíjense una cosa, ahí hay una sigla que es la GESIC, que al final ahora aprendí, porque es bastante larga, me costó aprenderla, pero todas maneras acá la miro por las dudas, es la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y de la Sociedad de la Información.

Esa agencia está ubicada en la Presidencia de la República, digo, para que se ubiquen desde el punto de vista de la organización estatal uruguaya y dentro de ella puse dos, porque son las que estoy hablando de ellas, pero tenía que haber puesto tres: La unidad de acceso a la información pública, la unidad de protección de datos personales y la unidad de certificación electrónica. Son tres unidades que son órganos integrantes de la GSIC, pero que los tres tienen desconcentración, no se asusten, porque yo siempre uso derecho administrativo, pero no voy a entrar en eso, ¿desconcentración qué significa? Asignación legal específica de estas tres unidades que ni la Presidencia de la República ni nadie se la puede quitar, en propia, es privativa, desconcentración privativa.

Y cada una de estas unidades tiene tres miembros, pero uno de ellos está en las tres unidades, que es el director ejecutivo de la GSIC, que en este momento es el ingeniero *Plastornik*, como dije antes, somos tres miembros.

Entonces, estas unidades son presididas anualmente por uno de los otros dos miembros, en este momento me toca a mí, pero el año que viene si vuelvo, no voy a ser el presidente, vieron que acá dice miembro, porque cuando me invitaron era miembro y ahora soy presidente y el año que viene, eso es una característica de dualidad bastante uruguaya desde el punto de vista de no unificar demasiado a la autoridad, el poder y una persona física determinada, una tendencia nos dijo que siempre se cumpla o que se cumpla bien.

¿Cuál es la competencia de la unidad reguladora y de protección de datos? Perdón, prefiero referirme antes al punto de la absoluta autonomía técnica. Es desconcentrado privativamente, pero la propia normativa legal dice que no podemos recibir órdenes ni instrucciones de ningún tipo de nadie y eso, por supuesto, es un tema jurídico, pero es un tema ético y que depende del jerarca, pero depende de uno también si es el integrante, es un problema humano, pero subrayo el aspecto ético que en realidad también está en todo esto, no es un tema sólo de gobernanza electrónica en cuanto a la E, sino también ética.

En cuanto a las competencias. Tiene competencias de asesoramiento, de dictado de normas, de registro de bases y de código de conducta, puede autorizar transferencias internacionales de datos cuando no se da con las condiciones que dijimos antes del principio de continuidad.

Controla de oficio o ante denuncia de interesados y tiene potestad sancionatoria, observación, percibimiento, multa, suspensión de bases de datos hasta cinco días y en cambio para la clausura de base de datos se requiere decisión judicial.

Tenemos también un consejo consultivo integrado por cinco personas o cinco miembros que son representantes del Poder Judicial, del Poder Legislativo, que no tiene que ser un legislador en actividad y que además esté vinculado o sea experto en temas de derechos

humanos. Un representante del Ministerio Público, o sea, de fiscales; uno del área académica que en este momento es alguien de la Universidad de la República, del Instituto de Informática; no es la doctora *Brián*, que me gustaría que fuera ella ya que está acá, porque es del Instituto, pero no es ella en este caso, es una colega amiga también, y un representante del sector privado que corresponde a la Cámara de Comercio.

El estar centrado o ubicado, mejor dicho, dentro de la GSIC implica que a GSIC aporta, digamos, la base o el apoyo tecnológico, apoyo digamos, servicios de sensibilización ciudadana, servicio que puede prestar para los otros sectores, pero se dan cuenta que hay una ligazón entre el acceso y la protección de datos, como que funcionamos separadamente, pero a su vez conjuntamente de alguna manera y lo voy a volver a señalar.

¿Cuáles son los objetivos y a la vez retos permanentes de nuestra unidad, de la unidad de protección de datos?

Generar conciencia del derecho y de sus garantías. O sea, el involucramiento del ciudadano y la participación, la difusión, la promoción del derecho, la capacitación de los responsables, las buenas prácticas, el contribuir a una aplicación equilibrada en relación a otros derechos, entre otros, al derecho al acceso a la información pública y al interés público, porque también a veces en este tema existen –entre comillas- “choques” o pueden existir con ejercicio de las atribuciones de las autoridades públicas que en realidad son deberes poderes, tienen poderes porque tienen deberes que cumplir.

Posicionar al Uruguay también como país competitivo y la cooperación con otras autoridades que expresamente lo dice nuestra ley.

¿Cuáles son los avances que han tenido el Uruguay y oportunidades?

En primer lugar, quiero señalar, y ya fue dicho por Isabel Davara, etcétera, hoy incluso, la adecuación. O sea, fue declarado con nivel adecuado por la Unión Europea en una decisión del 21 de agosto del 2012.

De manera que como ya se dijo en el panel anterior, no necesitamos reglas corporativas vinculantes, ni cláusulas contractuales con respecto a la Unión Europea o a los países que la Unión Europea declaren que tienen ese nivel.

Uruguay ratificó el Convenio 108 de Estrasburgo y de su protocolo adicional que también fue nombrado y en este momento es el primer país europeo, que integra el Consejo de Europa y una representante de nuestra unidad participa en este mismo, creo que ahora en este mismo mes tiene que volver a Estrasburgo, ir a Estrasburgo para modificaciones que se están haciendo al Convenio 108.

Uruguay fue sede de la XXXIV Conferencia Internacional en Punta del Este en el 2012; ha participado, y para mí esto es importante, quizás por mi formación profesional de abogado, en cuanto a ajustes normativos; ajustes normativos respecto a la propia ley nuestra, en cuanto a sanciones.

Ahora salió un decreto, hará 10 días, en que se modifica en cuanto a las inscripción registral, para hacerla más sencilla y que no haya problemas y se pueda hacer *“on line”,* sin ningún cuestionamiento o problema, ni tenga nadie que ir ni siquiera a pedir información, cosa que ya se hacía, pero se facilita más.

También es la participación de otras normativas.

A veces nosotros tuvimos, nosotros decimos “un encontronazo”, algún choque con algunas entidades, por ejemplo, con el Banco Central que lleva la Central de Riegos Crediticios que pretendía que no estaba comprendida en nuestra ley contra nuestro criterio que la sancionó y contra criterios judiciales en el mismo sentido. Pero al final se concluyó en otra ley que tiene algún aspecto especial, pero parte de la base de que la Central de Riego Crediticio del Banco Central se sujeta a la Ley de Protección de Datos.

Otro ejemplo en materia del sistema de área social integrada del Ministerio de Desarrollo Social, etcétera.

También campañas escolares a las que refirió incluso la Comisionada Presidenta del IFAI ayer. Hicimos unas campañas muy interesantes el

año pasado y este año de niños de escuelas públicas y privadas, haciendo comics, tendría que haberlos traído acá, que era más lindo que estas presentaciones mías, con la base de justamente cuáles son las ideas claves. El respeto por mí, por ti y por todos, tus datos no son públicos. La intimad implica respeto a la libertad.

Y viendo los comics de los chiquitines, que si ustedes entran a la página nuestra, los pueden ver. Realmente yo diría que es una delicia desde el punto de vista de protección de datos, usando una palabra en virtud de quiénes son los involucrados, en este caso los niños, y a través de los niños las familias desde todo punto de vista.

¿Cuáles son ejemplos de temas relevantes considerados? Por razones de tiempo no me voy a referir a todos ellos. Pero, por ejemplo, en relación al acceso a la información pública, porque justamente lo que dije antes es que esa organización institucional hasta ahora nos ha servido en cuanto si están involucrados temas de las dos unidades, en la medida de la relación que tenemos se, digamos, si no existe urgencia no nos pronunciemos hasta escuchar la otra unidad y eventualmente a sesionar juntos, juntos pero separados, porque formalmente no integramos una única unidad.

En ese sentido, por ejemplo, hemos tenido consultas sobre becarios de Fondo de Solidaridad, sobre refugios sociales. Legisladores departamentales que querían saber con nombre y apellido quiénes eran atendidos como refugiados, en los refugios departamentales. Estaba bien que se supiera el origen de qué zona vienen, pero no el nombre y el apellido, etcétera, etcétera. Por razones de tiempo que ya me han pasado la tarjetita amarilla no voy a entrar. Pero también el derecho al olvido, que estoy de acuerdo totalmente con lo dicho ayer por José Luis Rodríguez, en cuanto a que es una expresión del derecho de cancelación y de oposición.

En nuestra ley expresamente se prevé como derecho, el acrónimo ARCO no incluye todo lo que en realidad la legislación nuestra comprende, y creo que las otras también.

Y en nuestra ley se refiere expresamente al derecho de inclusión y también al derecho de supresión, emplea esa palabra.

Hemos tenido temas, por ejemplo, alguna persona funcionaria pública, que servidora pública se diría acá en México, que está muy bien. Nuestra Constitución dice que el funcionario está para servir a la nación, así que está perfecto el del servidor público.

Que alguien hizo una denuncia ante una comisión parlamentaria con su nombre y apellido, y en la versión escrita sigue apareciendo, pero en la página del parlamento también está. Y la persona desea que la saquen.

Ahí no es un problema de los motores de búsqueda, sino directamente del editor que además no tiene obligatoriamente. Creo que lo hablamos con Jesús ayer, de tener una información en la página.

Es diferente en la publicación que corresponde al papel de la comisión parlamentaria.

Hemos tenido otros casos. Videovigilancia es un tema interesante también, que se ha planteado la relevancia de existir políticas de privacidad, de que se trate de un sistema subsidiario, qué plazo de conservación se tiene. Incluso se nos ha planteado. Ayer me hubiera gustado conversarlo con la Comisionada, que es profesora de Derecho Laboral, Patricia ¿no?

Que fíjense videovigilancia que se ha planteado por padres que quieren controlar mediante ese sistema a las empleadas cuando quedan con sus hijos en la casa solas.

Y es legítimo, pero tendrá que saberlo la persona, y por otra parte no usarse, supongamos, en baños o en lugares por el estilo.

O sea, el sistema de videovigilancia no es solamente, como uno piensa a veces, para proteger el derecho de propiedad o la seguridad de las personas, si no puede tener mayor amplitud en la relación laboral, y distintos tipos, temas de spam también, etcétera.

Hemos adoptado distintos criterios y modalidades de actuación, voy a saltar algunos, o sea, la importancia de las inspecciones y el secreto profesional; nuestra Ley prevé sanciones, jurídicamente no voy a

entrar a esto, pero no prevé las inconductas o la falta, vamos a llamarlo, las infracciones.

La unidad reguladora nuestra, lo ha determinado, se ha hecho un listado de ese tipo y digamos, tiene que existir un principio de proporcionalidad y la adecuación y de motivación, cuáles son las infracciones y las sanciones.

Un instructivo para transferencias internacionales, distintos materiales disponibles, resoluciones y dictámenes, guías sectoriales para educación, administración, telecomunicaciones, etcétera, learning para funcionarios y docentes, sistema de denuncias on line, etcétera.

Tengo números de detalles aquí, pero creo que no corresponde que entre en ello.

Les diría, para finalizar, siempre con esa visión que he tratado de referirme a protección de datos y acceso a la información pública, que primero que se da un funcionamiento armónico de las dos unidades y que transparencia, privacidad y control se revelan paradigmas conciliables en la teoría y la práctica.

En nuestro país lo está haciendo para que sea un verdadero estado constitucional de derechos, debe seguir siendo.

Muchas gracias.

Jonathan Mendoza Iserte: Muchas gracias, doctor Rotondo.

Agradecemos mucho que nos haya compartido la experiencia uruguaya.

A nuestro auditorio le recordamos que al final de las exposiciones de nuestros ponentes, tendremos una ronda de preguntas y respuestas, será hasta el final, y bueno, los exponentes cada uno de ellos tendrán un tiempo para poder responder en forma genérica, los cuestionamientos del auditorio.

Ahora damos la bienvenida a la maestra Lourdes Zamudio.

Es catedrática de la Facultad de Derecho de la Universidad de Lima, experta en la red Iberoamericana de Protección de Datos, y miembro fundadora de la Red Académica Internacional de Protección de Datos y Acceso a la Información.

Ha trabajado para diversas autoridades peruanas e instituciones del Estado como asesora en materia constitucional.

Fue agente del estado peruano ante la Comisión de Derechos Humanos, abogada por la Universidad de Lima, maestra en derecho constitucional por la Pontificia Universidad Católica de Perú.

Bienvenida, maestra.

María de Lourdes Zamudio Salinas: Muchísimas gracias.

Quiero también aunarme al agradecimiento al IFAI, que en su calidad de Presidente de la Red Iberoamericana de Protección de Datos, ha organizado este magnífico Décimo Segundo Encuentro de nuestra Red.

El modelo que nos ha asignado la Organización o el tema en realidad, es fundamental en la tarea de discusión en los emprendimientos regulativos o regulatorios que todavía en nuestra región se están dando.

Yo quisiera comenzar con una pequeña reflexión, referido al derecho a la protección de datos, como derecho fundamental de la persona.

La defensa de los derechos fundamentales, supone la defensa de la persona misma; pero el reconocimiento de estos derechos fundamentales, por las legislaciones internas, como por las declaraciones o convenios internacionales, para que no queden vacíos de contenido, requieren de medidas de garantía que logren que el ser humano cuando se vea afectado, amenazado, violado concretamente en sus derechos, pueda recurrir a ellos para atender y verse amparado en su pretensión.

Tradicionalmente los mecanismos que por ejemplo, al derecho a la protección de datos personales los ordenamientos jurídicos ofrecían,

estaban referidos a la acción de Habeas Data o en su caso a la acción de amparo, como demandas ante el órgano jurisdiccional y en muchos casos complementados con la acción de la defensoría del pueblo que como sabemos, tiene un poder de autoridad moral y no efectiva.

Estos mecanismos de protección han demostrado por lo menos en la mayoría de los contextos que no ha sido efectivos, por lo menos como garantía para un derecho fundamental.

Porque en realidad los mecanismos de garantía de los derechos deben responder a determinados principios, como el de inmediatez, asequibilidad, independencia, imparcialidad, efectividad.

Y entonces, cuando se ha regulado la materia de protección de datos desde sus orígenes, hemos podido apreciar en algunos casos de una manera más tenue, en otros casos de una manera más profunda y detallada, que ha habido referencias a una autoridad de control.

Y efectivamente, consideramos que la autoridad de control es la que puede garantizar la aplicación de estos principios y que puede a su vez, constituirse en el mecanismo de garantía efectiva para el derecho a la protección de datos personales.

Nosotros hemos tratado de estudiar el encargo del tema asignado a la luz de la autoridad de control administrativa, es decir, el modelo institucional para la protección de datos personales, centrado, concretado en la autoridad de control o de supervisión que las legislaciones o los estándares internacionales nos han venido proponiendo, sugiriendo.

En ese sentido, primero antes de referirme a un estándar internacional concreto, me parece pertinente señalar que los estándares internacionales buscan armonizar mínimos para la adecuada protección del derecho fundamental a la protección de datos personales en los distintos contextos estatales.

Estos estándares internacionales, por supuesto, son susceptibles de ser adicionados mediante determinadas medidas por cada legislación de cada país, como herramienta para una mejor protección del derecho.

Pero para entender mejor los estándares internacionales que existen, es importante tener en cuenta que ellos provienen de contextos diferentes, de continentes diferentes, de sistemas jurídicos diferentes, de entornos culturales diferentes e inclusive foros o grupos diferentes, aunque todos, por supuesto, buscan la protección adecuada del derecho fundamental a la protección de datos personales, valga la redundancia que corresponde.

Esto es, la misión de todos estos estándares es una efectiva protección del derecho, sin embargo, por las diferencias de su procedencia, vamos a darnos cuenta que los estándares no todos tocan los mismos tópicos y a veces cuando los tocan, lo hacen con un énfasis o un detalle diferente, dependiendo de cuál estándar es el que estemos considerando.

Sin embargo, es incuestionable el valor y la importancia de los estándares internacionales, como guías y orientadores en los emprendimientos regulativos que cada estado va asumiendo, también como mecanismos de interpretación de la propia legislación interna y para suplir los vacíos que puedan presentarse.

Hemos nosotros traído, sin pretender evidentemente ser exhaustivos, la referencia a algunos de los estándares sobre la materia que se han ido dando y que han hecho mención de una manera, como dije, tenua o un poco más detallada a una autoridad de control en la protección de datos personales.

En el caso de la OCDE, en 1980 con las directrices relativas a la protección de la intimidad y de la circulación transfronteriza de los datos personales, no pedía explícitamente una autoridad de control, situación que se modifica en el año 2013 con la recomendación del consejo relativa a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales.

En esta recomendación la OCDE sí no solamente reconoce la existencia de una autoridad, sino recomienda su configuración con poderes específicos.

En el caso de las Naciones Unidas en 1990 a través de la aprobación de la Resolución 4595 de su Asamblea General, en el punto ocho, sí detalla la necesidad de una autoridad de control responsable de supervisar la observancia de esos principios ahí aprobados.

Resalta también las garantías de la imparcialidad y la independencia de esta autoridad y también que en caso de violación a lo dispuesto en la ley o legislación nacional sobre la materia sea posible la aplicación de condenas penales u otras sanciones junto con recursos individuales adecuados.

Europa unos años más tardes a través de la Directiva 9546 del parlamento europeo y del consejo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, hay que considerar que esta directiva es la piedra angular en la que se basa toda la legislación sobre protección de datos personales para la Unión Europea y que se dio con dos objetivos: garantizar el derecho a la protección de datos personales y además garantizar la libre circulación de datos entre los estados miembros de la unión.

Esa directiva sí promovió la creación en cada estado miembro de autoridades de control independientes.

Podríamos referir ahí que el Artículo 28 directamente trata la autoridad de control para la directiva de la Unión Europea, se señala que los estados deben constituir una o más autoridades públicas en la materia, que estas deben ejercer sus funciones con total independencia, que además los estados miembros dispondrán la facultad o la competencia de la autoridad para ser consultada y evidentemente para poder opinar sobre las elaboraciones regulatorias o modificaciones normativas que afecten la protección de datos.

Esa autoridad de control para la directiva debe disponer particularmente de poderes de investigación, de intervención, capacidad procesal en caso de infracciones a las disposiciones nacionales, también atenderá las solicitudes de verificación de la licitud en el tratamiento, presentar periódicamente un informe y también la necesidad de cooperar entre las distintas autoridades de control.

En el año 2007 a nivel de la Red Iberoamericana de Protección de Datos que hoy nos congrega, se aprobaron unas directrices para la armonización de la protección de datos en la comunidad iberoamericana.

El objetivo de estas directrices era contribuir a los emprendimientos regulatorios que se estaban dando en nuestros países.

También, por supuesto, debemos mencionar a los estándares internacionales sobre protección de datos y privacidad de Madrid, acogida favorablemente por la XXXI Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en la ciudad de Madrid en noviembre de 2009.

Por ejemplo, esos estándares son más generales, porque tratan de abarcar a todo el mundo, y deben adecuarse a contextos diferentes, Red Iberoamericana, APEC, Unión Europea, y por lo tanto el desarrollo de los temas tienden a ser más generales.

Mencionamos también al proyecto de principios y recomendaciones preliminares sobre protección de datos personales del 2010 elaborado por la OEA.

También, me parece importante, referirnos a la propuesta de reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos, que en estos momentos está siendo debatido.

Este futuro estándar no, evidentemente por el año en que se da y por recoger toda la experiencia sobre la materia en el mundo desarrolla de una manera muy detalla las facultades y las competencias acorde a las exigencias de los tiempos.

Pero como todavía no está aprobada no vamos a referirnos más a ella.

Hemos escogido nosotros tres estándares para analizar qué nos dicen sobre el modelo institucional concretado en la autoridad de control o garante de los datos personales. Esos tres estándares están

constituidos por las directrices para la armonización de la protección de datos en la comunidad iberoamericana, en adelante directrices para la comunidad iberoamericana, los estándares internacionales sobre protección de datos personales y privacidad de Madrid de 2009, en adelante estándares internacionales de Madrid, y a nivel de la OEA proyecto de principios y recomendaciones preliminares sobre la protección de datos personales; del 2010 en adelante proyecto de principios y recomendaciones de la OEA.

En esos tres estándares vamos a analizar brevemente tres aspectos: naturaleza jurídica de la autoridad de control, competencias de la autoridad de control y las sanciones frente al incumplimiento de la legislación sobre protección de datos.

¿Qué nos dicen estos estándares sobre la naturaleza jurídica de la autoridad de control?

Bueno, las directrices para la comunidad iberoamericana, denominan autoridad de control, los estándares internacionales, autoridad de supervisión y la OEA nos dice autoridad responsable de la supervisión de cumplimiento de los principios sobre la materia.

Detalla, a diferencia de las otras dos las directrices para la Red Iberoamericana que las autoridades podrán tener personalidad propia o encontrarse integridad en la administración pública o en un organismo público existente. Dos caminos que se han seguido han sido considerados.

Además las directrices para la comunidad iberoamericana señalan que podrán tener como función exclusiva el cumplimiento de las normas de protección de datos personales o dar la alternativa de ejercer esa competencia sobre protección de datos junto con otras atribuciones que la legislación le asigne, como también vemos en algunos países.

Los tres estándares evidentemente señalan de manera clara y explícita que la autoridad debe actuar con plena independencia e imparcialidad.

En el caso de los estándares internacionales de Madrid y el proyecto de Principios y Recomendaciones de la OEA, detallen un poco más

cómo ayudar a esta independencia, por ejemplo, que la autoridad debe contar con la calificación técnica, las competencias suficientes y los recursos adecuados para conocer de las reclamaciones que le sean dirigidas.

En el caso de las directrices de la comunidad iberoamericana, de una manera más genérica se señala que deberán establecerse mecanismos que garanticen la independencia e inamovilidad de las personas, a cuyo cargo se encuentre la dirección de dichas autoridades.

¿Qué nos dicen esos tres estándares con relación a las competencias de la autoridad?

Bueno, la función de supervisión de la observancia de los principios sobre protección de datos personales, lo dice de manera explícita, los estándares internacionales de Madrid.

Las directrices para la comunidad iberoamericana y el proyecto de principios y recomendaciones de la OEA, señalan la facultad de la autoridad para manejar denuncias y atender las reclamaciones.

En el caso de las directrices de la comunidad iberoamericana, se detallan más las competencias. Por ejemplo, se señala que debe realizar las averiguaciones e investigaciones necesarias para el cumplimiento de las directrices, adoptar medidas necesarias para evitar la persistencia en el incumplimiento de esta normatividad, mantener un registro de los tratamientos llevados a cabo por los sectores públicos y privados, autorizar cuando sea preciso la transferencia internacional, esto también lo recoge los principios y recomendaciones de la OEA.

En el caso de las directrices para la región iberoamericana, promover mecanismos de autorregulación, dictaminar en proyectos de disposiciones normativas sobre la materia, la función de divulgación del contenido del derecho, la necesaria función de cooperación entre las autoridades, etcétera.

En cuanto a las sanciones, estos tres estándares señalan lo siguiente.

Evidentemente, como les decía, hay que considerar el contexto en que se dan estos estándares.

La OEA por ejemplo, en el 2010, señala que la autoridad debe estar facultada para prever reparaciones administrativas y menciona explícitamente que debe también estar en condiciones para emitir sanciones financieras por incumplimiento.

Acá hay una pequeña diferencia y voy a mencionarlo, porque ustedes pueden tener acceso a las directrices, para la comunidad iberoamericana, que cedieron en el 2007.

En ella se señala que la autoridad de control debe tener la capacidad para la imposición de las correspondientes sanciones.

Esta capacidad deberá o podrá estar en la misma autoridad administrativa o en los órganos jurisdiccionales.

O sea, en el 2007, esas directrices decían: La facultad de sanción puede estar en la autoridad de control administrativo o en los órganos jurisdiccionales.

Esto se dio porque en el año 2007 sólo teníamos una Ley General de Protección de Datos Personales, con una autoridad, con competencia en bases o bancos de datos públicos y privados, en Argentina y lo que se quería era en los diferentes contextos, promover la aprobación de otras leyes.

Hoy en día eso ya no sería, me parece en la mayoría de los casos, no basaría de un consenso a la autoridad de detener facultades sancionatorias para ser una garantía verdadera del derecho a la protección de datos.

Pero en todo caso en los tres estándares señalan que cuando la autoridad de control tiene la facultad sancionatoria, debe poder recurrirse a los órdenes jurisdiccionales en revisión de la decisión de la autoridad, lo cual sabemos que se concreta en el proceso contencioso administrativo.

Pues bien, ¿qué se desprende en relación al modelo institucional de la autoridad de control, de esos estándares analizados?

Con relación a su naturaleza jurídica, podrá ser una autoridad exclusiva en materia de protección de datos o una autoridad con competencia dual en protección de datos o en otra que normalmente es de transparencia y acceso a la información pública, algo que es sumamente claro, que la autoridad puede tener una personalidad jurídica propia o también la opción de que puede estar adscrita a otro organismo público ya existente. En lo que sí realmente es para todos válido y explícitamente exigido, es que la autoridad debe ser independiente e imparcial.

Y acá voy a relacionar el hecho de la, o sea, quiero tratar de encontrar una relación directa en la opción legislativa de tener una autoridad de control con personalidad jurídica propia a una autoridad de control adscrita como órgano a una autoridad administrativa o un organismo ya existente con el tema de la independencia necesario para la autoridad.

Yo no sé si puedo de acá el hipervínculo, necesito presionar en independiente para irme a un hipervínculo, si me ayudan por favor en lo que está resaltado y nos vamos a los ejemplos.

¿Qué ejemplos tenemos al respecto? Vamos a ir de más a autonomía a menor autonomía, ¿cómo se han recogido estos estándares o las opciones legislativas? Ponemos por supuesto al IFAI en primer lugar, porque gracias a la reforma constitucional de 7 de febrero de este año, es la autoridad de control que goza del máximo nivel de autonomía, porque es un organismo constitucional autónomo.

Evidentemente en estas condiciones la garantía de independencia no puede ser discutida ni cuestionada, pero podemos mencionar a España que no tiene un nivel de organismo constitucional autónomo, sino tiene un nivel de autonomía legislativa que se concreta en la Agencia Española de Protección de Datos y que nadie puede cuestionar, también la independencia y autonomía con que actúa.

Ahí podemos ir a la realidad argentina o peruana, que es mí país, donde vemos opciones legislativas que han incluido o han insertado

en la autoridad de control dentro de organismos públicos ya existentes, por ejemplo, qué hay en el caso peruano, tenemos al despacho ministerial, luego al despacho viceministerial de derechos humanos y acceso a la justicia y dentro de él, como órgano dependiente, la Dirección General de Protección de Datos Personales o la autoridad nacional de protección de datos personales peruana.

O sea, son varios caminos elegidos para garantizar un mismo derecho, en realidad al respecto podemos decir que no hay un modelo único a seguir, pero lo que sí debe quedar claro es que si no hay un modelo constitucional definido, la autoridad de protección de datos personales debe ejercer sus funciones con total independencia.

Esto va de la mano con que la autoridad no esté sujeta a instrucciones. Para que esta autoridad sea eficiente y efectiva debe ser autónoma e independiente, esto es, tener la libertad suficiente para cumplir adecuadamente sus funciones, para tomar las decisiones que le correspondan y también para tener el suficientemente peso dentro de la estructura del estado, porque también controla bases o bancos de datos públicos.

Ahora, por supuesto que hay que reconocer que los contextos políticos de muchos de nuestros países condicionan el nivel de autonomía con el que se dota a la autoridad y que también los avances en nuestra región en esta materia como en muchos otros, están condicionados considerablemente a las comisiones políticas de los gobernantes.

Si me ayuda a regresar a la palabra Perú, al hipervínculo por favor anterior. Estábamos nosotros analizando las conclusiones de los estándares con relación a la naturaleza jurídica y sus recursos.

También esos estándares nos están diciendo que las autoridades deben contar con mecanismos que garanticen la independencia, inamovilidad de las personas a cuyo cargo se encuentre la Dirección de Dichas autoridades. Están de la mano con las otras recomendaciones anteriores.

Había que analizar, hay distintas opciones legislativas en este aspecto.

Hay legislaciones que señalan un plazo de duración fijo para la autoridad y la forma de designación de la misma, donde intervienen diversos poderes del estado, como hay otras que la decisión es solamente de confianza, sin ningún plazo de inamovilidad, ni ninguna garantía en este sentido.

No podemos discutir en cuanto a la independencia de nuestras autoridades, pero las personas cambian. Y si la estructura definida legislativamente no garantiza o no favorece, pueden haber retrocesos.

También señalan esos estándares analizados, que la autoridad deberá contar con la calificación técnica, competencia suficiente y recursos adecuados.

¿Qué nos dijeron con relación a las competencias de la autoridad de control?

Bueno, esto es bastante común, supervisar el cumplimiento o la observancia de los principios en materia de protección de datos, así como el cumplimiento de la normativa, conocer las reclamaciones de los interesados, realizar investigaciones e intervenciones, autorizar cuando sea preciso la transferencia internacionales, de datos a estado que no garanticen el nivel de protección mínimo, promover los mecanismos de autorregulación, dictaminar sobre proyectos de disposiciones normativos, divulgar el contenido del derecho y cooperar con las otras autoridades de protección de datos.

En cuanto a las sanciones, todas.

Hoy en día debemos, yo creo que como consenso reconocer que deben tener capacidad para imponer las correspondiente sanciones administrativas por la violación del derecho, el incumplimiento de la normatividad sobre la materia.

Evidentemente el ser las máximas instancias administrativas de sanción, estas resoluciones de las autoridades deben ser recurribles ante los órganos jurisdiccionales.

Entonces no se concreta un modelo institucional específico. ¿Se debe ir hacia un modelo institucional específico en materia de protección de datos con relación a la configuración de la autoridad de control?

No, no se ha dado y no creo que se dé, porque las realidades son diferentes. Por lo menos la realidad nos indica eso.

¿Hay alguna tendencia al respecto?

Vamos a ver, con relación a las competencias exclusivas o a las competencias duales asignadas a la autoridad.

Tener una doble autoridad, una en materia de protección de datos y otra para el tema de Transparencia de Acceso a la Información Pública, ha sido seguida por muchas legislaciones en Europa y también en América Latina.

Tenemos que mencionar a España, Argentina, a Colombia a Chile y a Perú.

Vamos a ver cómo es esto.

En España tenemos la Agencia Española de Protección de Datos como autoridad de control, como materia exclusiva en protección de datos personales.

Y de acuerdo a la ley 19 del 2013, que aprueba la Ley de Transparencia de Acceso a la Información Pública y Buen Gobierno, se ha creado una autoridad en materia de Transparencia y Acceso a la Información Pública, denominada “Consejo de Transparencia y Buen Gobierno”, cuyo mandato estaría entrando en vigencia el 10 de diciembre de este año.

Otro ejemplo lo tenemos en Colombia.

Como sabemos, Colombia tiene como autoridad en Protección de Datos Personales a la Superintendencia de Industria y Comercio a través de una de sus seis delegatura, la Delegatura para la Protección de Datos Personales, y por la ley aprobada este año en marzo, el 6 de marzo la ley 1712, la Ley de Transparencia y de Derecho de Acceso a

la Información Pública le asignan al Ministerio Público la función de velar por el adecuado cumplimiento de las obligaciones sobre la materia. Dos autoridades diferentes con competencias diferentes.

En Perú, tenemos la Autoridad Nacional de Protección de Datos Personales dentro del Ministerio de Justicia, y no hay una autoridad en materia de transparencia, pero los proyectos que se han trabajado hasta la fecha el primero o el más importante presentada por la Defensoría del Pueblo, y los otros que vienen siguen de una manera más concreta. Esa propuesta es crear un Sistema Nacional de Transparencia y Acceso a la Información Pública o una autoridad para la Transparencia y Acceso a la Información Pública como ente rector en esa materia.

Puedo traer también a Chile a través de su Consejo de Transparencia, como autoridad en la materia, y si bien es cierto que hay un debate interno hay un proyecto presentado por el Ministerio de Economía, que ha sido sometido a consulta pública de una ley de protección de datos personales, que crea un Consejo para la Protección de Datos Personales, y esto se daría, se concretaría, en Chile tendríamos entonces la opción de una autoridad específica para la materia de protección de datos y otra, perdón, ya existe la autoridad para la transparencia y acceso a la información pública y se crearía la otra específica para protección de datos personales.

El siguiente modelo sería el de autoridad con doble competencia, es decir, un organismo dual. El modelo máximo lo tenemos acá en el IFAI, que tiene la competencia en protección de datos personales y también en transparencia de acceso a la información pública, y entiendo que El Salvador también en el Instituto de Acceso a la Información Pública es el órgano garante para ambas materias.

Sin duda cada opción legislativa que ha construido su modelo puede exhibir avances, puede exhibir limitaciones.

No hay recetas, hay experiencias que podemos compartir. Pero sí creo yo, y para terminar voy a señalar algunos retos que tienen esas autoridades de control, cualquiera sea la opción legislativa a la que ellos respondan.

En primer lugar el reto básico, desde mi punto de vista, es la educación que genere una cultura de protección de datos personales. Esto creo que es un problema común y recurrente en nuestros países, el desconocimiento de la población sobre la materia de protección de datos.

Y es claro que para que haya una sociedad donde se respete la protección de datos es necesaria la regulación, es necesaria la autoridad de control, pero no es suficiente, es necesario contar con personas, son ciudadanos que conozcan el contenido y el alcance de estos derechos.

Otro reto es el mejoramiento y fortalecimiento de la institucionalidad a través de los órganos consolidados como garantes de la efectiva vigencia del derecho a la protección de datos personales. Eso nos lleva a reflexionar en trabajar más en el tema de independencia y de autonomía que les permita a las autoridades utilizar de manera estratégicas sus funciones y atribuciones para poder consolidarse en sus sociedades.

También otro reto es contar con una estructura organizacional acorde con la magnitud de las funciones encomendadas, así como con los recursos humanos, económicos y logísticos suficientes.

Nunca va a ser suficiente, por ejemplo, el IFAI tiene este magnífico local, este magnífico edificio, tiene cerca de 600 personas que trabajan en él, y ahora como organismo constitucional autónomo con las competencias a nivel federal que tiene que requerir mayores recursos en todo aspecto.

Y salvando las grandes distancias, por ejemplo, nuestra autoridad en Perú, que hace grandísimos esfuerzos, sin duda requiere muchísimos más recursos para avanzar en esta tarea.

Otro reto importante es desarrollar nuevas estrategias que enfrenten con mayor eficiencia los diversos dilemas y contradicciones, originado por los cambios tecnológicos y el bajo nivel de conciencia del derecho.

En muchos casos, el desarrollo de la tecnología, supera las legislaciones sobre la materia de protección de datos. Entonces, las

autoridades tienen que ser creativas y desarrollar estrategias que le permitan cumplir sus funciones en esos entornos.

Y esto lo va a tratar la Sesión número siete más tarde, en este Encuentro.

La penúltima o el penúltimo reto que consideramos importante, es que las autoridades deben desarrollar una adecuada fiscalización que asegure el cumplimiento de las normas en la materia.

Desarrollar estratégicamente la fiscalización y también la aplicación eventual de sanciones, no solamente con la finalidad de sancionar, sino de educar.

Y por último, por la brevedad del tiempo, considero también que un reto fundamental de las autoridades, es asumir el rol que les compete, pero de una manera protagónica y dinámica, porque la autoridad de control en materia de protección de datos personales, debe ser promotora y garante de la vigencia y del respeto de la legislación sobre la materia.

Para estos dos importantes cometidos, debe desarrollar de manera estratégica, las funciones encomendadas, como las de capacitación, la de asesoría técnica, la de fiscalización, como hemos dicho, la eventual aplicación de sanciones a los titulares de los bancos de datos, a los responsables del tratamiento, y en su caso, a los encargados del tratamiento que sean renuentes, a cumplir la legislación sobre la materia.

En conclusión, podríamos decir que el reto de las autoridades de protección de datos personales, es no quedarse como autoridades a nivel de la letra de la Ley, sino lograr que las sociedades, donde ellas tienen competencia y las autoridades de sus sociedades, las reconozcan como verdaderas autoridades en esta materia.

Muchísimas gracias.

Jonathan Mendoza Iserte: Agradecemos la intervención de la maestra Lourdes Zamudio.

Nos acompaña también y le damos la más cordial bienvenida, al maestro Pablo Palazzi.

Es miembro del Colegio Público de Abogados de la Ciudad de Buenos Aires.

Profesor de la Universidad de San Andrés y socio del despacho Allende y Brea.

Impartió clases en la Universidad Católica Argentina en la Universidad de Australia y en la Universidad de Fordham, en Estados Unidos.

Fue asociado en el Estudio Morrison & Foster LLP, en Nueva York, donde se desempeñó en el Departamento de Propiedad Intelectual y nuevas tecnologías.

Abogado por la Universidad Católica Argentina, y maestro en derecho con énfasis en derecho de los negocios internacionales por la Escuela de Leyes de la Universidad Fordham.

Está especializado en las relaciones entre el derecho y las nuevas tecnologías y en propiedad intelectual.

Bienvenido, maestro.

Pablo Palazzi: Muchas gracias, Jonathan.

Bueno, me sumo a los agradecimientos a los dueños de casa, al IFAI, y a la red por este encuentro y por invitarme a participar en él.

Realmente me encantó la Sesión de ayer y aprendí un montón y escuché mucho y en la Sesión de hoy también.

Espero que también sea de su agrado.

Como prueba de lo que me interesó, casi llené el cuaderno completo de todo lo que dijeron.

El tema es hablar de tipologías y de sistemas de protección de datos, Lourdes ya nos habló y nos explicó con mucho detalle todo lo que está

pasando en la región latinoamericana en materia de autoridades, yo preferiría concentrarme en el modelo argentino para contarles un poco lo que está pasando y hay una serie de casos interesantes que se han tenido lugar hace poco en Argentina y están relacionados con la protección de datos y otros derechos que fueron sonadísimos que les voy a contar y previo a ello les voy hacer una breve introducción a la protección de datos personales.

En Argentina tenemos Habeas Data desde el año 94, luego en el año 2000 se aprobó una ley, que es la Ley de Protección de Datos Personales, no voy a entrar en detalle en la ley, pero para resumírselas le puedo decir que es una ley adecuada, o sea, que es una ley que es compatible con el modelo europeo de protección de datos, porque fue reconocida por la Unión Europea, fue el primer país, luego le tocó a Uruguay en la región.

En el año 2001 se aprobó un decreto reglamentario, en el año 2002 comenzó a operar la autoridad de protección de datos personales a la fecha tenemos 14 años de protección de datos, en estos 14 años la Agencia Argentina ha dictado más o menos 25 reglamentaciones que van del registro de base de datos, medidas de seguridad, sanciones, leyendas que hay que poner en el formulario de recopilación de datos, leyendas que hay que poner en el email con publicidad, un procedimiento sancionatorio y de auditoría lo que ha hecho que las empresas tengan que organizarse y tener un check list de cosas que tienen que tener ahorita para cumplir con la ley, bastante didáctico.

En materia de acción y educación hace tres años que la Agencia Argentina creó una cosa que llama Con Voz en la … que es un programa de educación para escuelas primarias y secundarias que contó un poco el (inaudible) y tiene algo parecido y lo que han hecho es que era un canal en YouTube, otro canal en Facebook y crea vías institucionales y van escuelas en la capital y al interior del país para educar a los menores acerca del uso de sus datos, creo que es algo muy importante como decía Nelson en el panel anterior, tenemos que buscar a los menores para que sean conscientes de los riesgos que tiene el uso que tienen de los datos personales y la Agencia Argentina lo hace con mucha didáctica, porque por ejemplo, tiene una especie de video donde está el lobo feroz y Caperucita Roja, pero actualizado a los datos personales y Facebook y toda una serie de alegorías con

cosas que la gente entiende en primaria, secundaria y todos los niveles.

Y actualmente la Agencia está trabajando también en dos resoluciones que por ahora son proyectos, uno es una guía o una serie de recomendaciones para fabricantes de aplicaciones móviles, para que tengan en cuenta elementos para que las aplicaciones no sean invasivas a la privacidad.

Y una segunda recomendación y posición para el tema de drones y la captación de imagen y datos en lugares públicos mediante drones o vehículos aéreos no tripulados, como se les llama. Ahora, ese es el panorama de protección de datos.

Ahora voy a pasar a los casos argentinos que quería comentarles un poco caracteriza lo que está pasando en Argentina. El primer caso que les quería comentar es un fallo de la, Corte Suprema Argentina de hace un mes más o menos, un caso que llama Belén, a María Belén Rodríguez contra Google, que era una modelo argentina que demandó al buscador, porque cuando se pidió el nombre de ella aparecía sus imágenes y su nombre asociados con sitios pornográficos, ella no tiene nada que ver con estos sitios y ha habido una gran discusión acerca de muchos temas respecto a este evento, era si Google, si los buscadores eran automáticamente responsables o antes había que notificarlos y ahora baja el contenido, se aplicaba el derecho de imagen, la Ley de Protección de Datos y esta es la parte un grupo de demandas, hay como 200 casos similares de modelos y celebridades argentinas que ya empezaron a retomar esto ya hace más o menos 10 años y recién se recibieron en la Corte Suprema.

El primer caso ocurrió por el 2004, cuando una Argentina que vivía en Canadá, se estaba por casar con su novio y a su novio le decía que era modelo. Y su novio la buscó en internet y lo primero que apareció es un montón de imágenes que no tienen nada que ver totalmente irreproducibles.

Entonces el novio dijo: -¿No me dijiste que eras modelo? -Esto no tiene nada que ver –le dijo- Esto está ahí, pero yo no lo puse.

Bueno, había páginas que habían usado el nombre de ella con formas para generar tráfico de esa página con el nombre de ella. Fue un abogado y el abogado presentó una cautelar contra un buscador y un juez ordenó remover eso.

El buscador apeló en el 2004 y la cámara confirmó.

Entonces todas las modelos empezaron a goglear y descubrieron que estaban en internet asociadas a sitios non santos. Entonces todas empezaron a presentar cautelares para que removieran del índice de buscador su nombre con esas páginas que no tienen nada que ver.

En algunos casos había imágenes verdaderas, porque había modelos que habían actuado en películas y había un desnudo y eran imágenes verdaderas. Pero en muchos casos eran imágenes falsas y era una falsa asociación entre estas páginas y las modelos.

Después de las modelos vinieron las *"celebrities",* que tampoco querían aparecer asociadas con ciertas cosas y aparecieron también funcionarios públicos, se presentó una jueza federal muy conocida y pidió que borren todo lo malo que había de ella en internet, pero ahí los tribunales empezaron a cambiar de rumbo y en vez de remover dijeron: "No, persona pública, funcionario pública, usted es un tema de interés público y no puede pretender que no se hable de usted en internet".

Y ahí la jurisprudencia empezó a cambiar y empezaron hacer dos cosas: A rechazar temas de interés público, de celebridades, está el caso de Diego Maradona, por ejemplo, que pidió una cautelar y le rechazaron ambas instancias. Maradona no quería que sacaran unos temas relacionados con su pasado, tema de drogas y también quiso sacar algunos temas de menores, que eso era más discutible porque Maradona tenía varios hijos y hay jurisprudencia en Argentina que ampara la publicidad sobre los juicios de filiación.

Pero como es una persona muy conocida, le dijeron que no lo podía hacer, como que se podía hablar de él, porque todo lo que sucedió alrededor de él es un tema de interés público.

Entonces se empezó a distinguir la jurisprudencia entre temas de interés público y personas famosas y el ciudadano común o las personas que eran modelos, pero que tenían cierta privacidad.

Pero después de las cautelares, que la jurisprudencia fue variando y afinando un poco el lápiz, vinieron juicios de daños, diciendo: “Me dieron la cautelar y la cautelar asumía que había prima facie, un dato falso, vinculado a mí. Bueno, ahora quiero que me paguen por daños y demandaron a Yahoo, a Google y en menor medida a Bing, que no se usa mucho, pidiendo daño por afectación de la imagen.

Y a unos tribunales aplicaron un criterio de responsabilidad objetiva, diciendo: Esto es automáticamente responsable, porque la informática y la tecnología generan un riesgo y, por lo tanto, el riesgo al desarrollo hace que todo sea una cosa riesgosa.

Y condenaron automáticamente a los buscadores.

Otros tribunales aplicaron esta responsabilidad subjetiva y dijeron: “No es automáticamente responsable el buscador, sino que es responsable de que tiene conocimiento”. Pero algunos buscadores tenían conocimiento y no removían, diciendo: “Esto es lícito, es legal, yo lo único que hago es reflejar lo que tiene una página web y yo indexo todo a la web”.

Entonces la discusión es: ¿Bueno, tiene conocimiento cuando alguna carta o documento o cuando sale ad cautelam diciendo que lo remueva? ¿O tengo derecho a esperar un fallo definitivo entre un tribunal de última instancia para ver si es o no legítimo? Porque si es legítimo, no lo voy a sacar. ¿Entonces desde cuando comienza esa responsabilidad subjetiva?

Todos estos temas llegaron a la corte, en este caso donde también se discutía si era violatorio al derecho de imagen el uso de buscador de imágenes.

El argumento es de la parte demandada decía: yo tengo derecho a la imagen, yo decido a quién le doy mi imagen, cada vez que el buscador de imágenes escanea mi imagen y la muestra a terceros está usando mi imagen sin permiso, por lo tanto viola el derecho a la imagen.

Y nosotros tenemos el derecho de la imagen en Argentina en la Ley de Derechos de Autor, como un artículo que está ahí medio escondido en la Ley de Derecho de Autor, porque no tiene mucho qué ver.

Y no hay muchas excepciones para el derecho de imagen. La única excepción es temas de interés público o consentimiento del afectado. Entonces no hay una recepción de esta nueva tecnológica que era el buscador de imágenes en el derecho de imagen argentino. Entonces el juez Decámara, que es un juez muy bueno, es un especialista en responsabilidad civil, condenó al buscado diciendo: mire, acá está la ley, el Derecho de Imagen, yo no encuentro ninguna excepción a la ley, debo condenarlo.

Cuando llega a la Corte la Corte dice un montón de cosas importantes, lo primero que dice es: No hay una obligación expresa de monitorear contenidos los buscadores. O sea, que no tienen que a priori revisar todo lo que tienen para sacar lo malo de lo bueno. Esto hace que no puedan ser automáticamente responsables, sino solamente porque tienen conocimiento efectivo, que es el segundo punto de la Corte.

¿Cuándo tienen conocimiento efectivo? Cuando hay una notificación fehaciente del buscador de esto. Esa notificación fehaciente se da cuenta de algunas formas, carta-argumento en donde le notifico de que tal URL hay algo que infringe ciertos derechos.

Y a partir de allí el buscador tiene que decir qué hace, y cómo hace para decidir, y bueno, ahora la Corte éste, en Estados Unidos le llaman notificación y retirada de contenidos.

Yo en el momento que hice le puse “notificación y retirada de contenidos con sabor argentino” porque es una distinción media rara. La Corte dice que lo tomó de Portugal, de un reglamento que implementa la directiva de comercio electrónico, que habla de contenido flagrante. Entonces cuando el buscador tiene conocimiento efectivo del contenido legal hay que distinguir si la infracción es flagrante, claramente visible y determinable con una simple visita al sitio lo tiene que remover inmediatamente. Si no es flagrante, si no es claro que es ilegal el buscador necesita orden judicial o administrativa.

Y acá es importante la palabra “administrativa” porque entra a jugar una agencia de protección de datos que puede pedir remoción de contenidos. Ahora vamos a ver un caso en que esto ocurrió, que se fallón en la misma fecha de fallo de la Corte. Entonces entra a jugar protección de datos, porque yo podría decir ahí había datos personales, en datos personales violan cierto artículo de la ley, remuévalos. Y el problema de los casos flagrantes es cuáles son, y la otra pregunta es ¿son sólo los que dijo la Corte? Porque la Corte dijo un montón, dijo casos donde hay clara discriminación racial o expresiones relacionadas con el genocidio, con el odio racional o religioso, insultos a una determinada religión.

El segundo caso es los fotomontajes, que es común en Argentina, novio o novia despechada que pública una foto que era privada, y cuando se pelean deja de ser privada y la pública en una red social. Luego la publicación de cosas que deben de ser íntimas, aunque no tengan contenido sexual, o sea que no es el caso de escenas íntimas de la pareja, de una familia o cualquier cosas. Por ejemplo, en Argentina es constitucional el consumo de estupefacientes en ámbitos privados, para el consumo personal.

Entonces una persona puede estar fumando mariguana en su casa, que es legal, y alguien lo fotografia, un amigo, y después eso se difunde. Pero en fin, esa es una acción privada. Cualquier otra acción privada que sea privada.

Otro supuesto es que serían privados que la Corte menciona el caso de pornografía infantil, es un delito la pornografía infantil, con lo cual escena de pornografía infantil es automáticamente un delito y lo tiene que remover. Pero ahí se agota. Todo lo demás tiene una zona gris que hay que ver. Pero ahí se agotan.

Todo lo demás tiene un nudo que hay que ver caso por caso, a ver si es flagrante y es obvio que uno con sólo verlo puede determinarlo o no.

Y acá entramos en derecho a la privacidad, personalidad y una zona gris, porque los ciudadanos tienen privacidad, las personas públicas también, pero en menor medida y en asuntos de interés público o personas públicas con temas públicos, no hay tanta privacidad.

Entonces, hay una gran discusión acerca de qué tienen que promover o no, ya la discusión va a ser esto entre la primera sección o en la segunda y necesito una orden judicial o administrativa.

El segundo tema se va a aplicar también a temas de derecho de autor, marcas y secretos comerciales y otras cosas que no sean derechos, está por aprobarse.

Pero el fallo bueno, por qué, porque protege la terminología, al mismo tiempo proteger también ciertos derechos donde claramente se requiere una solución y ahí aclara que no hay automáticamente una responsabilidad de los intermediarios.

El fallo se refiere a buscadores, pero para mí se aplica a cualquier otro intermediario.

Después el segundo caso que quería comentar, son dos casos de acceso a la información pública; en Argentina estamos al revés que México, empezamos con protección de datos y recién ahora estamos entrando a acceso a la información pública y no tenemos Ley Nacional de Acceso a la Información Pública.

Tenemos un decreto que se aprobó hace 10 años, pero es un decreto que lo hizo por el Ejecutivo en cualquier momento puede cambiar o revocarse.

Sin embargo, llegaron un par de casos hace dos años a la Corte, donde se pedía información patrimonial de entidades públicas; el Gobierno le venía negando que curiosamente usaba la Ley de Protección de Datos como excusa para negar esto, o sea, sistemáticamente la Dirección de Datos Personales decía que no se podían hacer datos a particulares, porque eran datos personales, y por lo tanto cualquier información pública que tuviera datos personales, no se podía dar.

Y en el primer caso que ha de ser contra spam y asociación de derechos civiles, una ONG que discute estos temas, la Corte lo declaró al derecho de acceso a la información, pero ya como un derecho fundamental, dijo que tenían que dar los datos, que no se tenía que pedir legitimación, porque lo podía pedir cualquier

ciudadano, y siguió un poco las directrices de la OEA, el fallo de la Corte Interamericana, que condenó a Chile en acceso a la información pública, y dio la verdad una interpretación amplísima del acceso a la información pública.

Fue tan amplia que yo me atrevo a decirlo, lo puse por escrito que en Argentina no necesitamos Ley de Acceso a la Información Pública, porque la Ley que salga seguramente algo va a limitar y los fallos de la Corte, son mucho más amplios.

Después de este fallo, pasó un año y vino un nuevo fallo, mucho más discutible, que demuestra de qué forma, qué amplia la Corte está interpretando el acceso a la información pública. Era un caso donde se pedía el listado completo de planes sociales, que el Gobierno estaba dando a la gente, con nombre y apellido y cuánto lleva cada persona, y bueno se dan planes a esa gente que no tiene trabajo, pero de repente hay personas que lo tienen por 10 años, a plan social, con lo cual que uno no consigue trabajo durante 10 años, es sospechoso.

Entonces, había sociedades, organizaciones de sociedad civil que discutían que no eran muy claro los planes, por lo tanto, querían saber para controlar.

El Gobierno dijo: “No”, el que tiene un plan social es una persona con problemas. Por lo tanto, si yo digo que esta persona recibe fondos del Estado, lo van a estigmatizar porque es un dato sensible, no les voy a dar los planes; fueron a Tribunales, discutieron, ordenaron dar los planes y la Corte sacó este fallo donde los del acceso a la información pública están muy contentos y dicen es un logro.

La gente del sector de protección de datos dice que es una mancha negra para la protección de datos, porque dijo que la Ley de Protección de Datos, cuando habla de datos sensibles solamente son esos que están ahí mencionados, que no menciona planes sociales, o recibir un plan social y bueno, los que están en protección de datos, dicen: “No, esto se tenía que interpretar más amplio, porque no es solamente lo que está enumerado en la definición de datos sensible, es todo aquello que tiene aptitud discriminatoria y quien recibe un plan social, puede ser discriminado”.

La Corte siguió fallando a favor de acceso a la información pública, hace unas semanas sacó un fallo donde confirma la obligación de dar información sobre el registro de sociedades, cuando usted tiene una sociedad la tiene que registrar y nos estaban dando información de ciertas sociedades acusadas de estar en connivencia y actos de corrupción y la Corte obligó a dar esta información también a un diputado opositor.

En materia de acceso a la información estamos creciendo muchísimo a nivel judicial, nos falta una ley, se está debatiendo, pero como les digo, mi visión es que la necesitamos. Si está vendría mejor, pero como vienen los fallos para el acceso a la información pública es muy fuerte en Argentina.

Tercer caso. Es un caso muy interesante, porque es un caso que se origina en la Agencia Argentina de Protección de Datos, se trataba de un abogado que se estaba divorciando de su mujer y como parte de las peleas que había, la mujer lo acusó de abusar de sus hijos, entonces se hizo una denuncia penal, lo terminaron sobreseyendo porque no tenía nada que ver con esa denuncia, pero la ex esposa publicó la decisión en todas las redes sociales, en sitios, con lo cual cada vez que uno buscaba el nombre de esta persona en internet se encontraba con estos antecedentes de una denuncia penal por abuso de sus propios hijos, él probó la dirección que no tenía nada que ver, lo convenció la dirección y la dirección le pidió al buscador que elimine los contenidos que indexaban a esta persona, este era un caso de derecho debido, sino un caso de datos falsos. Lo aclaro porque la prensa, la gente confunde todo y siempre sacan el tema de derecho debido con este tema que no tiene nada que ver.

Y Google se defendió diciendo: No estoy acá, mi servidor está allá en California, por lo tanto no tengo que cumplir con Argentina. Los argumentos que ya hemos visto ayer y la dirección dijo: No. La búsqueda se hace por google.com.arg, yo le apunté ahí y está registrado que en Argentina, por lo tanto tiene base de datos acá y tiene que cumplir con la Ley de Protección de Datos Personales.

Google apeló este, agotó la vía administrativa y después se fue a revisar el acto judicialmente. Y ahora a fines de octubre salió el fallo de primera instancia, cálculo que se ha apelado donde un juzgado de

primera instancia de lo contencioso administrativo valida la sanción de la Agencia de Protección de Datos de Argentina, que buen inicio, es el primer caso donde un Tribunal argentino valida en las facultades que tiene la Agencia Argentina para sancionar a un buscador y da una interpretación amplia del concepto de tratamiento y da una interpretación amplia también de la jurisdicción que tiene la Agencia Argentina sobre sitios de internet.

Incluso como anécdota cuento que el actual director de protección de datos de Argentina cuando salió el fallo, éste lo comentó, escribió un artículo en la ley validando todo esto y diciendo un poco, trayendo a colación el fallo del Tribunal Europeo del 13 de mayo y diciendo un poco que lo que se dijo allá fue aplicable por allá Argentina, aparecía la Española y a la Europea y, por lo tanto, aplicando este fallo un poco para usar términos futbolísticos: Quedó la pelota picando frente al arco y el arquero no está.

Digamos, todo lo pasó dejar acerca mucho más el derecho de (inaudible) que el fútbol en Argentina, porque ya dijeron que tiene jurisdicción la Agencia Argentina, que el tratamiento de datos, etcétera.

Con lo cual no sé, un poco hablando de convergencias, hay bastante seguimiento en Argentina de jurisprudencia europea y la Agencia Argentina cita mucho esos dictámenes, trabajo de *Working Part*, etcétera.

El cuarto caso que me parece interesante comentar es un caso que llama Chicas Bondy, señoritas, bondy, colectivo en Argentina, en no sé qué idioma. Y era un señor que les sacaba fotos a señoritas en el colectivo y las publicaba en su blog y llevaba un año sacando esto y la Agencia de la Ciudad de Buenos Aires de Protección de Datos inició una especia de causa, porque consideró que esto podía poner en juego la protección de datos personales.

Y esto trae a colación el tema de privacidad en lugares públicos.

Y la gran pregunta es: ¿Si existe privacidad en lugares públicos y cuánto?

Lo que hacía esta persona era sacarle fotos, y la persona fotografiada parecía que no estaba prevenida y le estaban sacando fotos, había como 500 fotos y la Agencia de la Ciudad de Buenos Aires de Protección de Datos invocó en un caso en un caso inglés de protección de datos que se llama “Peck contra Reino Unido”, que es un fallo del Tribunal Europeo de Derecho de Derechos Humanos.

Dijo que había privacidad en lugares públicos y que esto era una violación y que tenía que darle, que pedirle consentimiento y tenía que dar derecho de retirada.

Se habló con esta persona y me contó que tuvo un solo caso de periodo de remoción que lo dio de baja.

Pero aquí hay algo interesante, porque la Agencia Argentina de la Ciudad de Buenos Aires solamente tiene injerencia en sus registros públicos, que es la facultad que tienen las jurisdicciones locales.

Y bueno, no sé hasta qué punto puede emitir un dictamen que aparte no tiene facultades sancionatorias, simplemente mera recomendación sobre un particular que saca fotos y las pone en internet.

Es un caso interesante, porque muestra hasta dónde van las agencias de la tutela de datos personales.

Finalmente otro caso más que quería comentar, era un caso muy interesante, porque está relacionado con lo que comentaron ayer los comisionados de Colombia y de Perú, que es el tema de los sitios clandestino.

Argentina está lleno, ha de haber cuatro o cinco sitios que son sitios que ustedes ven, tienen datos del quit, del DNI, algunos tienen datos de registro automotor, se venden como empresa de informes comerciales, pero tiene muchos más datos que informes comerciales, tienen datos de vecinos, tienen un montón de información que uno se pregunta: ¿Dónde lo consiguen?

Cuando voy a ver, uno quiere hacer un periodo de acceso, no puede porque no hay nada.

Cuando va a ver quién es el dueño de la página, hay un “private juice” que es una forma de tapar a quien es el verdadero dueño del sitio.

Acá pasó con un caso en Argentina, que era el caso de Agloinfo, que era una empresa de informes comerciales, pero que tenía información extra, que incluiría informes de vecinos y la agencia lo sancionó porque consideró que tuvo muchas denuncias y consideró que no era necesario en un informe comercial incluir datos de vecinos, porque no hablaba de la capacidad económica de una persona.

Con lo cual era un dato desproporcionado, tampoco daba un espacio para que la gente pudiera pedir acceso y corrección. Entonces terminó sancionándolo.

Le pidió que rectifique todo, pasó un año y esta empresa sancionada no hizo nada. Entonces para tomar más cartas en el asunto, lo que hizo el anterior Director de Protección de Datos fue mandar una nota al “Nic-Arg”, que es la agencia argentina que registra nombres de dominio y ordenó dar de baja el dominio .com.arg.

Fue una medida bastante drástica, pero bueno, hay que reconocer que el sitio era clandestino, en realidad el sitio estaba registrado en la zona franca, en una sociedad que estaba registrado en la zona franca de Uruguay, con un único accionista que era una sociedad inglesa.

Tuvo una mecánica para esconder alrededor de un individuo. Se pregunta por qué si alguien hace negocios en Argentina tiene que esconder todo esto.

Y bueno, esto genera el tema de los datos clandestino y cómo en Protección de Datos lo vamos a ver cada vez más con esto y habrá que buscar mecanismos de interacción entre las agencias, porque con internet cualquiera con dos clic se esconde y es difícil que lo encuentren.

Así que eso es todo para el panorama argentino, tengo más casos, pero se me está acabando el tiempo.

Muchas gracias.

Jonathan Mendoza Inserte: Muchas gracias por su exposición, maestro Palazzi.

Finalmente, pero con igual importancia, damos la más cordial bienvenida al maestro Patricio Vallespín López, es Vicepresidente de la Comisión Bicameral de Transparencia de Chile. Desde 2006 es diputado por el distrito número 57. De 2002 a 2004 fue Intendente de la Región de Los Lagos, y entre 1999 y 2001 se desempeñó como Director Nacional del Programa Chile Barrio, y Director Regional de la Región Metropolitana de la Comisión Nacional de Medio Ambiente.

Fue asesor de empresas en planificación y gestión estratégica y consultor internacional en temas de planificación y gestión, descentralización y medio ambiente para la Corporación Técnica Alemana, la Unión Europea, el Banco Interamericano de Desarrollo y el Programa de Naciones Unidas para el Medio Ambiente.

Licenciado en Geografía y maestro en Asentamientos Humanos y Medio Ambiente por la Universidad Católica de Chile, tiene estudios en Economía, Planificación y Políticas Públicas, y Métodos de Planificación y Gestión Estratégica.

Bienvenido, maestro.

Patricio Vallespín López: Muchas gracias.

Siempre un desafío adicional exponer antes de la hora del almuerzo, así que trataremos de responder a ese desafío y agradecer la invitación del IFAI a este foro Iberoamericano de Protección de Datos Personales para compartir la experiencia de Chile en materia de modelos institucionales porque creo que en esto todos tenemos que aprender. Creo que acá todos nos vamos enriquecidos con nuevas reflexiones, nuevos aportes y en ese sentido señalar que como diputado en Chile hemos considerado fundamental que el Congreso de Chile pueda hacer un aporte en esta materia, y hemos constituido una comisión bicameral de senadores y diputados para abordar el tema de la probidad, la transparencia, el acceso a la información y esto nos ha llevado también a involucrarnos en lo que es la protección de datos personales, porque van profundamente de la mano.

Pero permítanme una breve irrupción, porque como diputado de Chile en representación de la Cámara de Diputados de mi país, creo que nadie puede perder la capacidad de asombro respecto de lo que pasa cuando se abusa de los derechos humanos.

Y es por eso que quiero expresar públicamente la preocupación por la desaparición de los 43 jóvenes en Iguala, acá en México, y manifestar como diputado de Chile nuestra máxima solidaridad con todas las familias de estos jóvenes, porque esta abominable acción, sin duda, un atentado a los derechos humanos que no tiene nombre, y que yo diría esperamos que el gobierno de México pueda esclarecer esta situación a la brevedad, pues los jóvenes no pueden ser víctimas de la violencia política.

La democracia, a mi modo de ver, se consolida cuando estos temas se aclaran y se resuelven de cara a la gente, y en ese sentido si no somos capaces de hacer estamos constituyendo una democracia incompleta, que no es capaz de garantizar a sus ciudadanos la seguridad.

Creo que ese es un tema que nunca debemos perder de vista, por tanto, de verdad, esperamos como Cámara de Diputados de Chile, que esto se aclare a la brevedad por el bien de México y de su gente.

Hecha esa irrupción entro de lleno ahora a la reflexión que me han pedido, y partir señalando que voy a hacer una reflexión y aproximación política, porque soy un actor político, y en esa línea voy a usar el caso de Chile para fundamental el por qué hoy estamos, es lo que voy a explicar hacia el final de mi presentación.

Si bien es cierto comparto lo que se decía ayer por uno de los panelistas que internet puede ser de verdad un aporte a la libertad de las personas, y un aporte también a construir una mejor democracia, no es menos cierto que también podríamos constituir una democracia incompleta, si no somos capaces de garantizar a todos los ciudadanos de nuestros países la protección de sus datos personales y de su privacidad en general. Si no están obviamente fallando las dos cosas. El desafío es cómo lo conciliamos.

Y en ese sentido para mí la protección de datos personales es un derecho humano, emergente, nuevo, que se relaciona con la dignidad de las personas cuando apenas nos decía otro expositor ayer, y en esa línea yo creo que nosotros no podemos perder de vista, como actores políticos, que debemos regularlo y defenderlo.

La libertad a mi modo de ver, se debe expresar con responsabilidad, y cuando hablamos de responsabilidad, ahí a mi modo de ver está el espacio de la acción política para la protección de datos personales, porque claramente tiene que ver con una decisión eminentemente política, porque se vincula con el tipo de sociedad que queremos construir, porque efectivamente, si los datos personales son considerados como un bien de consumo más, que se mueve en el mercado libremente, constituimos un tipo de sociedad distinta, donde eso se reforma en algo fundamental.

Distinta es cuando la protección de datos, queríamos que se transforme en un derecho social, garantizado por el Estado y yo estoy en esa visión, donde esto es un derecho social garantizado que debemos asegurar y que después técnica y tecnológicamente y jurídicamente debemos resguardar, pero ese principio rector no lo podemos perder de vista.

Por tanto, para mí es un tema netamente político e ideológico, no es un tema como también aquí algunos panelistas dijeron ayer, que es técnico, tecnológico, casi como de neutralidad, en el ejercicio de los derechos de las personas.

Yo creo que esto es exactamente un derecho que sí debemos regular y protegerlo en un contexto obviamente de innovación y avances tecnológicos permanentes, que dificultan, sin ninguna duda a la legislación y las normas, porque la legislación y las normas, normalmente es más estática que lo que es lo dinámico de las tecnologías y el Internet, pero que por el bien de los ciudadanos de nuestros países, lo debemos hacer.

Dicho eso, quiero reflexionar que en el caso de Chile, hoy queremos avanzar hacia un enfoque que parta, yo diría, o lo construyamos desde la libertad, la igualdad y la dignidad de las personas, que creemos que es muy distinto que cuando uno se aproxima a este tema de la

protección de datos, desde la mirada de la propiedad, porque obviamente se construyan sociedades distintas por una y otra mirada.

Y en este sentido, a modo introductorio, quiero señalar que como se decía también en la mañana por el expositor Esquenazi, son más ya de 70 países que han adoptado leyes para la protección de los datos personales, que están en manos de organismos públicos o privados, muchos de ellos también tienen legislación sobre acceso a la información pública y evidentemente en todas esas, se abordan también los datos transfronterizos, porque es parte del abordaje de esta temática.

En Chile, sólo a título inicial, porque después lo voy a abordar con un poco más de detalle, ya 1999 se dictó una Ley, la 19628, que regula la protección de datos personales, cautela la información que concierne a personas naturales, identificadas o identificables desde una perspectiva que pretende garantizar que sus titulares sean quienes deciden sobre su uso, conceptualmente bien encaminada.

El año 2008, casi 10 años después, se queda la Ley 20285, en la cual se norma el régimen de acceso a la información pública, es la información que obra en poder de los órganos del Estado, que puede incluir, por cierto datos personales, con la óptica de favorecer su conocimiento por parte de la ciudadanía, ese es el estado del arte general.

Pero permítanme hacer una reflexión sobre los modelos institucionales de la mirada, yo diría operativa, de cómo esto llevar a la práctica. Existen dos grandes áreas: Uno es la existencia de dos órganos garantes separados como se ha visto acá, uno destinado a garantizar el ejercicio del derecho de acceso y otro, hacerlo en relación al derecho de la protección de datos. Ahí tenemos entre otros casos, Canadá, Irlanda, Francia, Nueva Zelanda dentro de los principales.

Cuando hablamos de establecimiento de un solo órgano garante de las atribuciones y competencias tanto en materia de acceso a la información pública como de protección de los datos personales, ahí tenemos otros insignes representantes como Estonia, Serbia, Reino Unido y México que nos cobija en esta jornada.

Permítanme hacer una muy breve expresión de cuáles son las ventajas y desventajas para que el pueblo, actores políticos podamos tomar decisiones respecto a ello de ambos modelos, por una parte el de dos órganos garantes la ventaja que tiene es evidente que hay una existencia de referentes institucionales claros para avanzar y hacer efectivos ambos derechos, sin necesidad de equilibrar y resolver de antemano potenciales tensiones entre ambos.

Tiene la desventaja de posible surgimiento de conflictos interinstitucionales entre dos órganos, por lo que se recomienda muchas veces establecer mecanismos institucionalizados para la resolución de conflictos entre ambos órganos. Sin embargo, dado que en la práctica su funcionamiento no siempre es adecuado, también debería juntarse con acuerdos de cooperación entre los agentes, entre los entes garantes con la finalidad de minimizar conflictos entre ellos.

Obviamente aquí viene otra desventaja, que es el mayor costo de crear, establecer y mantener un órgano adicional el ejercicio de ambos derechos.

En materia de un órgano único aparecen algunas ventajas evidentes: Reducción de las posibilidades de conflicto interinstitucional, se resuelven adentro, si al órgano creado originalmente para garantizar un derecho se le suma una segunda función o tarea, se beneficia por cierto de la experiencia y experticia previa que se ha adquirido, hay otra ventaja también que facilita la tarea de lograr el equilibrio en el ejercicio efectivo de ambos derechos, hay una reducción también de costos administrativos tanto de recursos humanos como infraestructura y equipamiento.

Y también hay una disminución como ventaja de la posibilidad del mal uso de la protección de datos por parte de los organismos públicos, para negar acceso a información pública, al saber que sus decisiones serán revisadas por un órgano dotado de ambas competencias. Ese es como un catálogo de posibles ventajas.

Tiene la desventaja por cierto del riesgo de que un interés o derecho prevalezca sobre el otro o que el órgano no sea igualmente efectivo en la protección de ambos derechos o en equilibrarlos en forma óptima y en esto creo que la presentación de la representante de Perú,

Lourdes, ha sido bastante clara en mostrar lo que se ha hecho en cada uno de los países en esta materia.

Dicho ese análisis de las posibles institucionalidades, la situación vigente en Chile con un poco más de detalle. La ley 19100628 de 1999 entregó a los tribunales de justicia el conocimiento y la resolución de las reclamaciones que se presentaren en esta materia.

En teoría esta ley estuvo bien encaminada, pues se reconocía al titular de los datos el derecho de acceso, el derecho de modificación o rectificación, el derecho de cancelación y el derecho de bloqueo.

Pero la práctica nos ha demostrado, y por eso estamos convencidos que hay que cambiarla a pesar de que no hayamos tenido éxito todavía en 100 años de discusión.

Por qué nos damos cuenta que al no existir una institucionalidad adecuada para garantizar estas garantías, de alguna u otra manera no se están dando como corresponden, ni tampoco hay un sistema de sanciones que permita de alguna u otra manera resguardar adecuadamente su vigencia como ley.

Y por otra parte, se creó el … Bueno, el resultado de lo anterior, quiero ser muy claro también a mi modo de ver, que ha existido un debilitamiento de las garantías constitucionales respecto de la protección de los datos de las personas.

Por otra parte, la Ley 20285 del año 2008, sobre el Acceso a la Información Pública que creó el Consejo de la Transparencia, que ya tenemos al ex presidente del Consejo de la Transparencia para Chile, don Jorge Jara, que mañana va a compartir con muchos de ustedes la experiencia de Chile y los avances en esa materia, que es un organismos autónomo, como lo decía la señora Lourdes, de promover la transparencia y la función pública.

En forma indirecta, y esto es lo importante, le entregó la atribución de velar por el cumplimiento de las normas de la Ley Sobre Protección de Datos Personales por parte de los órganos de la administración del estado.

Esto lo ha hecho, a nuestro modo de ver, bastante bien, porque el número dos del Artículo 21, una de las causales de rechazo a la entrega de información consiste en que su publicidad afecte los derechos de las personas, particularmente tratándose de su esfera de vida privada, circunstancia que puede ser evaluada por el consejo.

Si el solicitante de la información pública que quería saber, denegada, recurre ante él solicitando amparo a su derecho de acceso.

El Artículo 7 también señala que el Consejo debe velar por el cumplimiento de la normativa relativa a la publicación en los sitios web institucionales de cierta información que pudiera incluir datos personales, por ejemplo, a cerca del personal, de los proveedores, de las personas que reciban transferencias de fondos públicos, etcétera.

En la práctica el Consejo de la Transparencia explicitado en esta ley dicta instrucciones generales en materia de transparencia, qué datos personales pueden ser publicados y cuáles no, formula recomendaciones específicas para su tratamiento y resuelve los casos sometidos a su conocimiento.

Según la información que yo puedo acceder, se estima que cerca de la cuarta parte de las decisiones de fondo que ha tomado este Consejo para la Transparencia, tienen que ver en mayor o menor medida con datos personales.

Dicho esto y que eso ha funcionado yo diría bien en materia del Consejo para la Transparencia, algunos caninos que Chile ha explorado para avanzar en modificar y perfeccionar la ley del año 99, ya se los comenté, que tenemos un claro diagnóstico que hay que mejorarla, pero no hemos sido capaces de avanzar en su desarrollo y su promulgación final. Y en eso aquí con Raúl Arrieta también que es mi asesor del Ministerio de Economía que está redactando el proyecto y que en vamos en diciembre a iniciar la discusión legislativa, hemos muchas veces coincidido en promover cosas que asegure la protección de los datos personales y muchas veces también bloqueando o torpedeando los argumentos que el gobierno, el que sea, a veces ha puesto sobre la mesa de discusión.

En este sentido, quiero señalar que en octubre del 2008, por ejemplo, el gobierno de… era aparte, el primer gobierno de la Presidenta de Chile, que hoy nuevamente está de Presidenta se presentó una ley para modificar la Ley de Protección de Datos Personales, donde lo que buscaba era transformar al Consejo para la Transparencia en el Consejo para la Transparencia y la Protección de Datos Personales. Vale decir tener las dos funciones en un único órgano.

De manera tal de supervisar ambas regulaciones. Esto finalmente no avanzó. Hay un grupo parlamentario, entre los cuales me contaba, que queríamos avanzar en tener un órgano específico, especializado, diferenciado y la disposición se atrancó y ese proyecto está en el baúl de los recuerdos.

En paralelo varios parlamentarios hicimos iniciativas legislativas, tanto senadores como diputados de reforma constitucional para crear una agencia de protección de datos, que optaba por el modelo de dos órganos por separado.

Obviamente requerimos que el gobierno dijera la hacemos nuestra y la ponemos en discusión, porque es de iniciativa exclusiva del Ejecutivo. Tampoco convencimos hasta el 2010 a nuestro gobierno, avanzar en esa línea y esas iniciativas también quedaron en el baúl de los recuerdos.

Pero qué ha significado. Que vamos consolidando posiciones respecto a la materia.

En junio de 2011, y ahí ha existido siempre coincidencia, ha sido bastante más fácil avanzar en Chile, en avanzar en acceso a la información, más transparencia, más entrega de información. Se modificó la Ley del Consejo para la Transparencia, rectificando algunas de sus normas y creo que hemos perfeccionado bastante su modelo.

En enero de 2012 el gobierno pasado, del cual yo era oposición, presentó el proyecto de ley que regulaba el tratamiento de los datos personales, establecía procedimientos de reclamo más expeditos y equilibrados para los titulares de datos respecto de los responsables

encargados del tratamiento, complementaba el actual procedimiento judicial de reclamo con dos instancias administrativas previas.

Una si se trataba de reclamos en contra de organismos públicos, las partes podrán reclamar de lo resuelto por el Consejo de la Transparencia a la Corte de Apelaciones y, por otra parte, en el caso de reclamaciones en contra de organismos privados crea una instancia voluntaria de entendimiento a través del servicio nacional del consumidor, que es una institución pequeña en Chile, que depende del Ministerio de Economía, que iba asumir esta situación previa al ejercicio de acciones ante los tribunales civiles.

Ante lo cual nosotros, también como parlamentarios de oposición, dijimos: por ningún motivo hay que seguir avanzando en esa línea, porque, punto uno, está restringiendo el ámbito de protección de los datos personales sólo al ámbito o del comportamiento de un actor económico en tanto cuanto consumidor y de protección de datos personales es mucho más que eso. Y además la ley hablaba de que miren: apliquemos esto por tres años y ahí vemos cómo seguimos. Eso era inaceptable, porque la protección de datos personales tiene que ser un tema mucho, mucho más importante.

En esa línea nos damos cuenta que como no tenemos todavía un cuerpo legal aprobado y promulgado, si uno analiza lo que ha pasado con propuestas de diputados y senadores, hay más de 70 mociones parlamentarias relativas a la protección de diversos aspectos relacionados con la protección de datos personales que ejemplifican la preocupación que tenemos como legisladores en esta materia, no sólo por los estándares impuestos por la OCDE, sino también por la acción muy fuerte de numerosas organizaciones de la sociedad civil que demandan mayor protección de los datos personales y su consagración como un derecho humano fundamental y que quiere en la Constitución de la República de Chile, que además vamos a tratar de cambiarla en el actual Gobierno.

Dicho esto, ¿en qué estamos hoy? Y ésta es la opción que Chile está queriendo tomar, por lo menos de quiénes somos partidarios de este enfoque que el Gobierno ha recogido.

El Ministerio de Economía, hoy está elaborando un proyecto de Ley de Protección de Datos de las personas, del tratamiento de los datos personales en detalle, cuya finalidad es crear un sistema de protección de datos sustentado en el derecho de las personas de controlar y proteger su información, de manera de evitar que sus derechos sean afectados por el tratamiento de los datos.

El anteproyecto éste recoge la experiencia y la discusión nacional que se ha dado en esta materia, en el Congreso Nacional, como en los tribunales de justicia de manera de dar un salto cualitativo en el estándar de protección de los derechos de las personas, adaptando a Chile a las exigencias que las relaciones internacionales, tanto políticas como económicas y comerciales, exigen para mantener integrado nuestro país al mundo, considerando la tradición jurídica chilena que somos bastante legalistas.

Este proyecto de ley que se está por presentar, la verdad es que ha considerado una gran variedad de experiencias que ahí están explicitadas, en el caso de la resolución de Madrid, directivas de la Unión Europea, de la OCDE, el caso de la experiencia legislativa española, el caso de la Ley Estatutaria de Colombia, de también de Costa Rica, Uruguay, México, la Unión Europea, etcétera, un conjunto de antecedentes que probablemente nos estamos demorando más, pero quizá vamos a ser una mejor legislación y su texto y esto es muy importante, ya hemos incorporado a los ciudadanos en esta discusión, fue objeto lo que llamamos en Chile una consulta ciudadana.

Raúl Arrieta que armó este proyecto lo subió a la página web del Ministerio de Economía, y ha estado en análisis varios meses que terminó en agosto y esto significó que se recibieron más de 650 observaciones y comentarios aportes a esta reflexión que tenía plena coincidencia respecto a que es fundamental avanzar en esta materia y que hay que abordar esto con una institucionalidad ad hoc y que se fortalezcan el sistema de garantías en materia de protección de datos.

Eso igual es una muy buena noticia, pero significa que estamos bien sintonizados.

¿Cuál es el objeto? Y aquí lo voy a decir muy brevemente, porque vamos a dejar la presentación, ¿cuál es el objeto de este proyecto de

Ley? Garantizar el derecho de las personas naturales de proteger y controlar la obtención, tenencia, tratamiento y uso y transmisión de los datos personales que le conciernen de modo de lograr un adecuado recuadro de los derechos de la Constitución Política, asegura a todas las personas, regulando también la transferencia internacional de datos personales.

Pero este proceso de consulta ya ayudó a perfeccionar esta parte, y esto ya lo vamos a expresar ahora de una manera mucho más potente a nuestro modo de ver, que va a ser garantizar y proteger los derechos de las personas que emanan de su dignidad, libertad e igualdad, respecto del tratamiento de sus datos personales, de modo de, y esto es lo importante, de lograr el resguardo de sus derechos constitucionales reconocidos.

Ahí van a estar temas tan importantes como se destaca el hecho de la protección de datos personales, es un derecho irrenunciable, se requiere para el uso de los datos personales, el consentimiento inequívoco y para el caso de datos sensibles, inequívoco y expreso, y también se señala que jamás el tratamiento de los datos personales, puede atentar contra los derechos humanos de las personas, lo cual nos parece que es bastante potente en su planteamiento.

Obviamente hay exclusiones de la ley, como en todos los países, para aquellas que son netamente informaciones del ámbito de la vida privada, familiar, para aquellos temas que tengan que ver con finalidad, bases de datos de seguridad, inteligencia, defensa nacional, obviamente están excluidas del contenido de esta Ley.

Las bases de datos creadas y reguladas por leyes especiales en temas no sé, lo que sea, terrorismo, narcotráfico, que sé yo qué. Y el tratamiento de datos personales que se realiza en el ejercicio de las libertades de emitir opinión y de informar.

Y respecto al tema institucional creo que llevamos un paso fundamental por tanto yo soy un firme defensor de esta propuesta que se va ingresar, que se crea el Consejo para la Protección de Datos. Será una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio, como lo decían que era fundamental que había de considerar.

Su objeto es promover y garantizar el derecho a las personas naturales de proteger y controlar los datos personales que le conciernan, fiscalizar el cumplimiento de las normas generales y especiales sobre el tratamiento de datos personales.

Tienen un catálogo de funciones del Consejo donde me gustaría resaltar algunas: Velar por el cumplimiento de la normativa relativa al tratamiento de datos personales por parte de organismos públicos, privados y personas naturales, también entraron al tema, de personas naturales.

Asistir y asesorar obviamente a las personas naturales que lo requieran, respecto de los alcances de la normativa relativa al tratamiento de datos personales. También, por cierto, dictar en su caso, sin perjuicio de las competencias de otros órganos del estado las instrucciones que permitan los organismos públicos, privados y personas naturales adecuar el tratamiento de datos a los principios de la ley, pudiendo adquirir ajustes y en general un conjunto de funciones que le van a dar la fuerza suficiente para poder proteger de verdad los datos de los ciudadanos.

Por cierto, que va colaborar otra institución, otras instituciones van a tener que colaborar con su actuar, pero no para debilitar la acción de protección de datos personales si no llevara enriquecerlo.

Y para que vean la importancia de la consulta ciudadana previa, la composición que inicialmente el anteproyecto de ley decía lo que estaba ahí, hoy lo hemos cambiado, porque hemos escuchado y acogido estas peticiones y vamos a buscar un sistema de una composición de cinco miembros con un presidente, abogado designado por el Presidente de la República, pero elegido de una terna, de una quinta, perdón, armada por la Corte Suprema, estamos involucrando a todos los poderes del estado en esta tarea fundamental.

Dos consejeros abogados y dos no abogados de los cuales dos serán designados por la Corte Suprema y los otros dos por designación del Presidente, pero con aprobación mayoritaria del Senado de la República, incorporar a todos en la designación.

Los cinco serán elegidos además por un curso de oposición de antecedentes y con dedicación exclusiva con inhabilidades amplias y pertinentes, porque queremos darle realce a esta instancia, porque queremos que la protección de datos es un tema que no podemos debilitar en quienes se dedican a esto.

El periodo de los consejeros durarán seis años a su encargo, pudieron ser designados sólo para un nuevo periodo, se renovarán por parcialidades de tres años, el Presidente será designado por la presidenta, como ya dijimos, por los cuatro años. Va tener autonomía e independencia que es muy importante, se va crear también en esta ley un Registro Nacional de Base de Datos que nos parece fundamental para nosotros, creo que eso es importante.

En Chile hemos visto cómo las bases de datos se venden al mejor postor y creemos que ahí hay que hacer una regulación de esa materia y el Consejo deberá inquirir y registrar esas bases de datos y actuaciones, siendo notificados todos los actores pertinentes, por cierto que vamos a tener una administración del Registro Nacional de Base de Datos que el Consejo deberá dictar las instrucciones que fijen el procedimiento, obviamente infracciones y sanciones y se derogarán las leyes vigentes para esta materia y, lo más importante, la adecuación de base de datos que inicial se había pensado para un año, se van a dar tres años, de manera tal que se adecúe a las nuevas normas.

Y termino solamente señalando que es evidente, como hemos visto en este evento, que ambos derechos pueden y deben armonizarse a través del mecanismo de la ponderación de derechos, para lo cual existen distintos enfoques y soluciones institucionales que acá muchos han contado y que el der echo comparado las respalda, desde las que promuevan la existencia de una sola entidad que aborde ambos temas o por separado.

Lo importante, y eso es el rey de la condición, yo diría, que cualquiera que sea el modelo que se adopte, la clave está en la autonomía e independencia de la o las autoridades garantes y en la suficiencia de las potestades y de recursos humanos y financieros para cumplir sus funciones y obviamente la generación, como lo decía también

Lourdes, de una cultura de protección que en el sistema educativo se debiera implantar.

Por tanto, como decía, y termino con una reflexión política final, hay que transformar, a mi modo de ver, en un derecho social garantizado y la protección de datos personales. Pues a mi modo de ver, incide en el tipo de sociedad que queremos construir.

Una sociedad de ciudadanos conscientes de sus derechos en materia de protección de datos o una sociedad de funcionarios obedientes, que vean a los datos personales como un bien más que se trance en el mercado y que fluya a todos lados sin ningún tipo de regulación.

Y creo que a mi modo de ver no es el camino indicado, porque no debemos olvidar nunca que el grado de desarrollo de las democracias modernas se mide por la capacidad de los estados, de defender y proteger los derechos de sus ciudadanos.

Y la Protección de Datos Personales, a mi modo de ver, se marca en ese enfoque.

Muchas gracias.

Jonathan Mendoza Inserte: Muchas gracias, maestro Vallespín López.

Damos inicio a la sesión de preguntas y respuestas

La mecánica propuesta es cinco minutos para cada uno de los ponentes, para responder los cuestionamientos planteados.

Por orden de exposición, iniciaríamos con el doctor Felipe Rotondo.

Felipe Rotondo Tornaría: La mía va a ser más breve, porque es una pregunta sola, no es para cinco minutos.

Me preguntan sobre la videovigilancia, tiempo de conservación, tipo de consentimiento que se requiere.

Brevemente que me refiera a eso.

Yo dije algo, pero muy rápidamente. Se requiere una política de privacidad de la seguridad de las imágenes, son datos. Por lo tanto, debe ser inscrita en el Registro de Base de Datos y allí especificarse y consignarse cuál es la finalidad.

Si es para una finalidad determinada, no debe usarse para otra cosa, obviamente. Si es una finalidad sobre obra pública, no puede utilizarse para una finalidad diferente que encontraría al principio de especificación básico en materia de protección de datos.

También es importante, creo que lo dije, el principio de veracidad.

Entiendo que no puede ser sino, diría subsidiario el sistema de videovigilancia y no de principio.

Claro, vinculado con el consentimiento y esto de manera general por la Ley de Protección de Datos.

Si hay casos en que no se requiere el consentimiento, si está vinculado a la seguridad pública perfectamente. Pero entonces ahí tiene que tener la línea determinada precisamente que es para eso, no para otra cosa y los principios restantes rigen.

Ayer dijo algo el amigo José Álvaro Quiroga, de Perú, que me gustó mucho, aunque quizá va fuera de esta pregunta, en el sentido de que aunque se trate de datos de acceso público no significa que dejen de regir los restantes principios.

Entonces aprovecho la ocasión para apoyarlo, aunque de alguna manera no se refiere directamente pero sí está involucrado aquí.

Como tienen que inscribirse en el registro de nuestra unidad, nuestra unidad hizo un distintivo, un logo respecto a la videovigilancia. Si algunos de ustedes van a Montevideo en la mayoría de las empresas de transporte público, está en los buses de Montevideo, porque tiene que aparecer la indicación de la base de datos quién es el titular, el lugar para ejercer los derechos ARCO, o sea, quién es el responsable. Eso figura en el propio logo. Que no significa que deba imponerse ese

logo, pero lo que está contenido allí sí; o sea, puede variar un poquitito, pero siguen usando eso.

Y con respecto al consentimiento, si se trata de base de seguridad pública no se requiere. Ahora en Montevideo, por ejemplo, en la zona del centro en la ciudad vieja, los amigos argentinos, veo a Pablo, pueden conocer bastante esa zona. Además es linda, vale la pena. No creo que tanto como la zona del Zócalo de acá, pero de todas maneras.

Y ustedes saben que había problemas de seguridad pública, y la videovigilancia ha servido mucho.

El tema está en que ha tenido que ser mejorado ese sistema, pero no desde el punto de vista de protección de datos, sino tecnológico, porque agarraban a los supuestamente delincuentes, los llevaban al juez y el juez no estaba convencido a través del sistema de las imágenes para identificar con plenitud a la persona. En este momento se ha logrado mejorar eso. Pero va más allá del tema que estoy hablando yo.

O sea, en el sentido de que puede no requerirse el consentimiento para determinados sistemas de videovigilancia.

También en el caso que yo nombre del trabajo, o sea, no se necesita el consentimiento si se trata de, existe una relación contractual o una relación laborar, pero que lo requiera necesariamente. O sea, eso es importantísimo que necesariamente se requiera para cumplir la relación contractual o la relación laborar ese requisito.

En ese caso podríamos decir que no se necesita el consentimiento, pero sí el conocimiento. O sea, el conocimiento, en ese caso como dije antes que puede ser discutido la cuidadora del niño o de los niños en la casa particular de alguien.

De manera que no hay duda que allí se necesitaría, sin duda, el conocimiento previo y, por otra parte, lo podría hacer, y creo que lo dije cuando hice mi presentación, en todos los lugares de desempeño de la persona.

Con respecto al tiempo, el tiempo es un tema clave junto con la finalidad. De todas maneras no existe normativa que refiera a un tiempo. Acá fue un principio, no aparece en nuestra legislación como principio.

Pero es un principio general de derecho, el principio de razonabilidad. Todas las personas tienen que actuar razonablemente en la aplicación de las normas.

Existe el Contralor Judicial o Jurisdiccional si corresponde, pero evidentemente no se puede tener ese caso de videovigilancia de la empleada, por ejemplo. O sea, debe requerirse de acuerdo a las circunstancias, no puedo dar una norma general, pero está vinculado al resto de los principios.

Básicamente creo que hasta ahí.

Jonathan Mendoza Iserte: Muchas gracias, doctor.

Por favor, maestra Lourdes Zamudio.

María de Lourdes Zamudio Salinas: Muchísimas gracias por las preguntas.

Hay una que señala en su opinión: ¿la transparencia y acceso a la información pública, debe estar separada del órgano garante de protección de datos?

Ni los estándares internacionales definen este tema, ni las opciones legislativas van en un solo sentido.

Acabamos de escuchar a Pablo Palazzi, que él considera que no debe haber una Ley de Acceso a la Información Pública, y entiendo, tampoco un órgano garante. O sea, no hay una definición en la materia de que deban estar o no separadas.

Lo que hay que hacer, me parece, es analizar el avance de ambos derechos y las medidas de garantías de esos derechos en el Estado concreto.

Y a la luz de lo que dicen los estándares internacionales, configurar si deben estar en una autoridad dual, con competencia dual o separada.

Ayer mismo en la Sesión final de este Encuentro, vimos cómo los senadores han expresado su voluntad en el sentido de que el IFAI mantenga la competencia sobre las dos materias.

O sea, no hay una respuesta definitiva, hay que analizar en virtud a la realidad concreta.

A su criterio resulta incompatible que la autoridad que gestiona y administra un sistema de registros públicos, pueda ser la misma autoridad de protección de datos personales.

Me parece que ha habido intentos en este sentido. El sistema de registros públicos, en algunas legislaciones, se señala que tiene su propia normatividad, no obstante se rige por los principios de la Ley General de Protección de Datos.

Quizás conversábamos con Felipe, no sería la opción más adecuada.

Otra pregunta señala: Los principios constitucionales hablan de división de poderes y sistema de pesos y contrapesos.

Al designar al IFAI como único órgano garante ¿no estaríamos vulnerando dichos principios? ¿Quién sería el contrapeso del IFAI?

Y me ponen una frase: el poder corrompe y el poder absoluto corrompe absolutamente.

A ver, en realidad este principio constitucional es la base del estado liberal que viene a modificar la primera forma de estado moderno que es el estado absoluto para separar o evitar el absolutismo de los monarcas que concentraban todas las funciones del Estado en una sola mano.

Hoy en día, la división de poderes, es un principio que como tal, división de poderes, en realidad el poder del Estado es uno sólo, no se divide, se habla de las funciones asignados a distintos órganos del poder.

Pero hoy en día, los estados son muy complejos, tienen millones de habitantes. Lo que existe a la par o en respuesta a esta complejidad, es una serie de organismos constitucionales autónomos, con competencias exclusivas y excluyentes, que además en un estado constitucional de derecho tienen funciones señaladas por Ley y el principio de legalidad se aplica, la autoridad actúa, hasta dónde pueda, le permita y necesite para cumplir las funciones legalmente o constitucionalmente asignadas.

Ninguna autoridad está exenta de una fiscalización en el caso de la autoridad administrativa, como el IFAI, sus resoluciones administrativas por un lado, van a ser o pueden ser revisadas ante el Órgano Jurisdiccional, pero por otro lado, la función administrativa, como altos funcionarios que son, también tiene una reglamentación y está sujeta a disposiciones o está sujeto eventualmente a sanciones administrativas.

La verdad es que no tengo, no he leído el estatuto del IFAI en cuanto a las eventuales sanciones o responsabilidad de los funcionarios, pero toda autoridad pública, un estado constitucional de derecho debe responder y siempre hay mecanismos de control o fiscalización. La ciudadanía es un mecanismo importantísimo y sé que ya lo han estado haciendo en algunos temas controversiales.

Hay otra pregunta, ¿cómo abordar el reto de fiscalización cuando en la actualidad en México, salvo honrosas excepciones, sólo se da cumplimiento a los principios de información y consentimiento? Hay una afirmación absoluta acá.

Yo creo que la respuesta es compleja en el sentido de analizar por qué si se diera esta situación que en realidad quizá en alguna medida, pero no totalmente, México tiene una experiencia en esa materia y para América Latina hay que considerar que sirve también como alguien que ha estado marcando en cierta forma la pauta de manera tal que si esto ocurriera tal cual lo señala en México, en otros países el cuestionamiento sería más absoluto si es posible.

En ese sentido, hay que ver por qué se daría este incumplimiento, los principios son lo fundamental, porque guían la actuación de los

responsables, del tratamiento y los encargados del tratamiento, sirven para llenar vacíos legales, sirven para interpretar la legislación y guían a los responsables del tratamiento, como digo, a los encargados.

Entonces, ¿qué falta? Difundir el derecho, sus alcances, entonces hay una tarea que cumplir en ese sentido. Sí hay que fiscalizar, hay que ver la capacidad y los recursos que tengan.

Me acuerdo hace un par de meses que estábamos en una empresa importante en Perú que pedía, estaba solicitando, ya había aceptado el proceso de adecuación, yo iba como una asesora de la empresa que había asumido este tema y un directivo muy importante dijo: Y esa autoridad que existe, dijo, ¿cuántas personas hay, qué capacidad tiene para fiscalizarnos? Porque si no, para qué nos apuramos, dijo.

Entonces, eso está en el pensamiento de muchas personas, sobre todo en los primeros años entiendo de aplicación de una ley, de vigencia de la autoridad, habrá que hacer, ver mis recursos y desarrollar fiscalización estratégica. Dependerá de ver los sectores que más incumplen o en los cuales puedo yo como autoridad dirigir estrategias de fiscalización, para que sirvan para recomendar el mejor cumplimiento de la norma, pero también que sirvan como docencia, porque lo que la ley quiere y la autoridad no es sólo aplicar sanciones, es que se inserte y se implante la cultura de protección de datos personales y eso parte de acciones preventivas y no tanto sancionatorias.

Hay una última pregunta que se refiere a Perú. ¿Tiene información de las sanciones impuestas en el Perú y si se han hecho efectivas y en qué medida, quién las cobra, si hay relación entre sanciones y cumplimiento?

En este tema la autoridad ya ha aplicado algunas sanciones, la ley tiene calidad, la autoridad capacidad de cobro coactivo, pero más allá de eso me permiten remitirme a lo que nuestra autoridad, el doctor José Álvaro Quiroga, expuso ayer sobre este tema y también hacer recordar nada más que la aplicación de sanciones supone en todo momento, pero sobre todo con la autoridad comienza actuar para ganar legitimidad, a estar sumamente sustentadas para que sirvan de

referente y de guía a todos los responsables encargados del tratamiento.

Muchas gracias.

Jonathan Mendoza Inserte: Muchas gracias, maestra.

Por favor, maestro Pablo Palazzi.

Pablo Palazzi: Hay dos preguntas que son del caso de los planes sociales. Así que las contesto juntas.

Creo que no se entendió bien el caso.

Era una ONG, se presenta ante el Ministerio de Desarrollo Social de Argentina, invoca el decreto de Acceso a la Información Pública, y le dice: “Deme el listado de todos los planes sociales que ha recibido la gente con nombre y apellido de los beneficiarios durante los últimos “n” años”.

Obviamente que había planes sociales de toda clase, o sea, gente que recibía compensación del estado por no trabajar, gente que estaba incapacitada para trabajar, gente que estaba en situación de vulnerabilidad, que reciben ayuda social. Es muy amplio el concepto de plan social, pero obviamente que son datos personales y son datos personales de personas y en algunos casos pueden ser datos sensibles.

El estado se defendió con la Ley de Protección de Datos Personales y dijo: “Son datos sensibles, son datos personales, no los puedo dar sin consentimiento de cesionario”. Son un montón de beneficiarios, lo cual era imposible conceder el consentimiento y la Corte falló a favor del Acceso a la Información Pública.

¿Por qué?

Porque tenemos un decreto que es Acceso a la Información Pública, tenemos una Ley que es Protección de Datos Personales, pero la Corte dijo: “Acceso a la Información Pública de derecho fundamental y está por encima de la de Datos Personales”.

Dijo que las excepciones al Acceso de la Información Pública eran de interpretación restrictiva, con lo cual minimizó un poco, o sea, terminó ganando la Ley de Acceso a la Información Pública, el régimen.

¿Por qué pasó esto?

Hay que entender un poco el contexto. En Argentina hacía cinco años que el gobierno usaba la Ley de Datos Personales como escudo para no dar datos de carácter público.

Entonces el listado es enorme, pero estaba el caso de contratos de servicio público, contratos administrativos que por su pura esencia son datos públicos. Acá en la mesa los especialistas de derecho administrativo, cualquier contrato administrativo en principio, con el listado le va a pagar plata a alguien o es algo público, es un tema patrimonial.

Esto también es un tema patrimonial, porque el estado le va a plantear a alguien.

Había casos, por ejemplo, donde se pedía quién fue a visitar a un ministro para hacer una reunión.

Decían que eso era privado, porque eso era un dato personal de la persona que había visitado al ministro y obviamente hay un registro de audiencias públicas y se tenían que haber revelado.

Incluso está el caso del sueldo de la presidenta, que se negó a darlo convocando a la Ley de Protección de Datos Personales, o sea, un montón de situaciones donde cosas que eran públicas se privatizaban bajo la Ley de Protección de Datos Personales.

Entonces en este contexto la Corte falló del lado de la Transparencia, porque sentía que estaban tironeando mucho la Ley de Protección de Datos Personales.

Entonces es un fallo que decide bajo la Ley de Acceso de la Función Pública que no hay defensas y minimiza el concepto de dato personal.

A la Agencia Argentina no le gustó mucho el fallo, porque el concepto de datos sensibles salió en el fallo de la corte, perdió fuerza. Obviamente hay que interpretarlo en este contexto, para que a través del próximo caso de datos sensibles la Corte no diga esto y falla con los datos sensibles.

Después me preguntan: ¿Qué hacen los buscadores después del fallo de la Corte que creó este sistema de ratificación y bajada de contenidos?

No sé, pero el fallo es de 28 de octubre. O sea, que es muy reciente.

Lo que pasa ahora es que hay que interpretar el fallo y ver cómo lo obligan los tribunales.

Hay contenidos claramente ilícitos que van a tener que dar de baja inmediatamente y otros que vamos a tardar cuatro años hasta que salga el fallo de la Corte de vuelta, a ver si eso no fue dado de baja.

¿Qué opinión le merece que en México no exista un Registro Nacional de Bancos de Datos Personales en posición de los particulares?

En Argentina tenemos un Registro de Bancos de Datos, donde se tienen que registrar todos.

En Europa la directiva de notificación de tratamiento es una forma más suave de decirlo tal vez, Registro parece una palabra muy burocrática y mi experiencia cuando tiró una empresa se registre me dice: No, no me quiero registrar.

Si hacemos notificaciones, hacemos una notificación on line y algo muy simple, yo lo veo mucho más fácil y creo que va ser mucho más efectivo y esto tiende a dar cierta transparencia en el tratamiento de datos personales, a veces no se entiende.

Pero fíjense que entre ayer y hoy vimos tres casos en Argentina, en Perú y en Colombia, de tratamientos clandestinos de datos personales, donde estas empresas o sitios fantasmas que no están registrados.

Entonces, el Registro le da más transparencia, cierto que también tiende a tener una tendencia burocrática y me parece genial esta solución de Uruguay de hacer el registro on line, es mucho más simple, este decreto que comentabas. Y en Argentina ojalá y lo hagan así más flexible porque creo que se registrarían muchos más, pero esa es la finalidad del Registro, creo que es bueno.

Hace poco salió un fallo que dijo que era constitucional registrarse en Argentina, pero fue validada la facultad de la Agencia de obligar a registrar.

Otra pregunta. De acuerdo al modelo argentino, es un tema si el estado recorre sitios de internet para evitar que haya sitios de contenido sexual, pornografía infantil, trata de personas, es un tema más de delitos informáticos, ¿hay una Fiscalía Especializada en Delitos Informáticos en la Ciudad de Buenos Aires, se va crear una ahora en la provincia de Córdoba y tal vez algún día una a nivel nacional? Y sí, las fiscalías actúan efectivamente y se encuentran en algunos sitios cosas de pornografía infantil, las denuncian y empiezan de oficio acciones.

Y hay dos proyectos de ley en Argentina para darle facultades al INADI, para contenido discriminatorio y una ley de trata para también dar de baja contenidos relacionados con trata.

El problema de esto que si bien es bien intencionado, hablan de ahora baja contenidos en redes sociales, de buscadores y no sé, es como que van a empezar aparecer un montón de organismos que van a tener que regular la red y yo lo veo complicado, porque fíjense en el ejemplo de las redes sociales, el *Hate Speech* en Estados Unidos es constitucional, pero Facebook es la red social por excelencia, podría haber permitido *Hate Speech*, pero elevó el nivel de protección y dice: No, el discurso basado en el odio racial no lo vamos a permitir, porque consideramos que es malo.

Entonces, activamente da de baja páginas de Facebook que tengan contenido por odio racial. Entonces, hay un tema de autorregulación que es bueno que funcione y darle facultades al gobierno para que allá baja sitios, a veces es complicado, que es (inaudible) argentina con un proyecto de leyes. Gracias.

Jonathan Mendoza Iserte: Muchas gracias, Pablo.

Daríamos el uso de la voz al maestro Patricio Vallespín y posteriormente habría un comentario adicional del doctor Felipe Rotondo, para concluir ya con esta mesa.

Patricio Vallespín López: Muchas gracias, la verdad que me llegaron una pregunta que era para dos, yo voy a responder por el caso de Chile.

La pregunta dice: ¿Existe alguna disposición en alguno de sus países que obligue a inscribir los registros del manejo de datos personales? Ejemplo, dice, si una empresa tiene un inventario en sus bases de datos, ¿debe inscribirlo ante el organismo oficial que se encargue de la aplicación de la Ley de Protección de Datos?

Yo decía que a veces la ventaja que tiene de no tener actualizada la legislación de protección de datos que en nuestro caso es del 99, es que podemos desde la realidad ir construyendo una mejor norma y en ese sentido el proyecto de ley que vamos empezar a discutir en el Congreso, tiene considerado la creación de un Registro Nacional de Bases de Datos, que se tratará de un registro de acceso público, permanente, en el que el Consejo de Protección de Datos debería inscribir y registrar las bases de datos y actuaciones que les sean notificados por los organismos públicos y privados.

Por tanto, va haber un registro tanto de datos de titularidad pública, como de titularidad privada y ningún responsable o encargado de esas datos podrá poseer datos personales, de naturaleza diversa o distinta de los notificados al consejo e inscritos en el Registro Nacional de Base de Datos.

Vale decir, de alguna u otra manera nos vamos hacer cargo de la pregunta que hacía acá el asistente, porque creemos, y yo te lo digo con conocimiento de causa, porque la creatividad humana para el abuso en el uso de los datos personales es gigantesca.

En Chile ha circulado una base de datos por un bufete de abogados, en la cual se identifican trabajadores que siempre asumen roles de dirigentes sindicales en las empresas en las cuales han trabajado.

Con lo cual obviamente esa base de datos lo que está haciendo es una lista de trabajadores que van a ser desempleados permanentes, porque cuando terminan de ejercer su rol de dirigente sindical, pierdan el fuero en base a la legislación laboral, necesidades de la empresa que ya existe en Chile, lo van a despedir, va a entrar a esa lista, etcétera.

Obviamente que esos tienen otros caminos para judicialmente enfrentarlo, pero la creatividad humana es gigantesca para el abuso en el uso de datos personales.

Por lo tanto, creemos que esta base de datos, que este registro que vamos a crear va a salvaguardar a los ciudadanos de su abuso, porque va haber un ente rector que va a estar preocupados de que esas se usen bien.

Por tanto, creo que vamos en la línea correcta.

Y la verdad, yo agradezco mucho con este evento que ha estado, me doy cuenta que hay elementos que ratifican la línea que nosotros estamos abordando, hay otros que nos dejan todavía signos de interrogación. Pero para eso está el proceso con el Legislativo, que el Ejecutivo presentará su proyecto y nosotros en el congreso vamos a perfeccionarlo en su contenido, pero con el principio básico de lo que dije al comienzo.

Yo creo que este es un derecho que hay que garantizar, sí o sí lo veamos regular, porque si no efectivamente nuestros datos personales van a fluir como hoy pasa en muchos casos en Chile, de mano en mano, sin ningún tipo de control y regulación.

Muchas gracias.

Jonathan Mendoza Iserte: Muchas gracias, maestro Vallespín.

Concluimos con el comentario del doctor Rotondo.

Felipe Rotondo Tonaría: Gracias, moderador, pero no deseaba cambiar el régimen que se ha seguido hasta ahora. Era por lo que planteó Pablo Palazzi respecto a la necesidad o no de una legislación en materia de acceso.

Yo viendo lo que tú acabas de decir tengo mis dudas, porque si la jurisprudencia va por ese camino. O sea, en el Uruguay hemos tenido casos casi iguales a los que tú dijiste, pero se entendió que correspondía dar la información pero anonimizada, disociada de los nombres. Por ejemplo, beneficios sociales, estoy hablando de acceso de la información pública y la otra cara vinculada al derecho de los datos personales, pidiéndose a personas públicas estatales o no estatales datos de beneficiarios de becas, de beneficios sociales, de regiones de qué zona eran, de qué edades, esos datos estaba bien dárselos, pero querían también nombres y apellidos. Eso no se les dio, les dijimos que no se les diera y judicialmente se dio la razón de que no se les diera.

Digamos en el Uruguay se ha llegado a pedir, por ejemplo, legisladores que constitucionalmente tienen la posibilidad de pedir informes, le es más fácil recurrir a la vía del acceso a la información pública que esperar la vía administrativa para obtener datos, perfecto. La regla tiene que ser en el estado de derecho a la publicidad y la transparencia, el derecho público, porque es derecho público, porque va parea la gente, para el público y la publicidad, la regla es que no estamos en un ámbito de lo secreto, perfecto.

Pero los derechos no son absolutos, (inaudible) de la vida, no hay ningún deseo absoluto, ninguno de los que estamos hablando ni de protección, pero tampoco en exceso.

O sea, claro, hay que gente que abusa, se pedían por ejemplo, datos vinculados, lo mismo que tú dijiste, a qué gente recibía, qué persona recibía un Ministro, perfectamente. Si eran tan total, correspondía dárselo, pero también pedían el teléfono particular del Ministro, eso no corresponde darlo.

Perdón, no quería demorar, pero como era muy parecido lo que tú planteaste Pablo.

Jonathan Mendoza Iserte: El maestro Palazzi, iba hacer uso de su derecho de réplica propiamente.

Pablo Palazzi: Cien por ciento de acuerdo, creo que la Corte tendría que haber anonimizado los datos ahí y se acabó el problema. Pero quería aclarar algo respecto de lo que dijo Lourdes, que yo no quiero una Ley de Acceso a la Información Pública en realidad. Lo que quise decir es que el fallo de la Corte es tan amplio que podríamos vivir sin la Ley de Acceso a la Información Pública, porque la Corte le dio todo a los que pedían acceso a la información pública.

Obviamente es mejor que tengamos una ley y también está viviente un organismo por el tema de que es más fácil acceder a los datos con la ayuda de un organismo público, no tener con un abogado litigar cuatro años. Pero en el contexto actual el fallo es buenísimo.

Jonathan Mendoza Iserte: Muchas gracias.

Presentador: A nombre de las comisionadas y comisionados del Instituto Federal de Acceso a la Información y Protección de Datos, hacemos entrega a nuestros ponentes de un reconocimiento por su valiosa participación en este Décimo Segundo Encuentro Iberoamericano de Protección de Datos Personales.

Entrega este reconocimiento y este obsequio Jonathan Mendoza, quien es el director general de verificación del Instituto Federal de Acceso a la Información y Protección de Datos.

Agradecimiento reiterado a los ponentes por su participación. Y a todos ustedes les informamos que dará inicio un receso en este momento, la hora de la comida, la próxima sesión será a partir de las 16:00 horas, a las cuatro de la tarde y les hacemos una cordial invitación a que sean puntuales para no retrasar el trabajo de este Encuentro Iberoamericano de Protección de Datos Personales. Buen provecho.

- - - o0o - - -