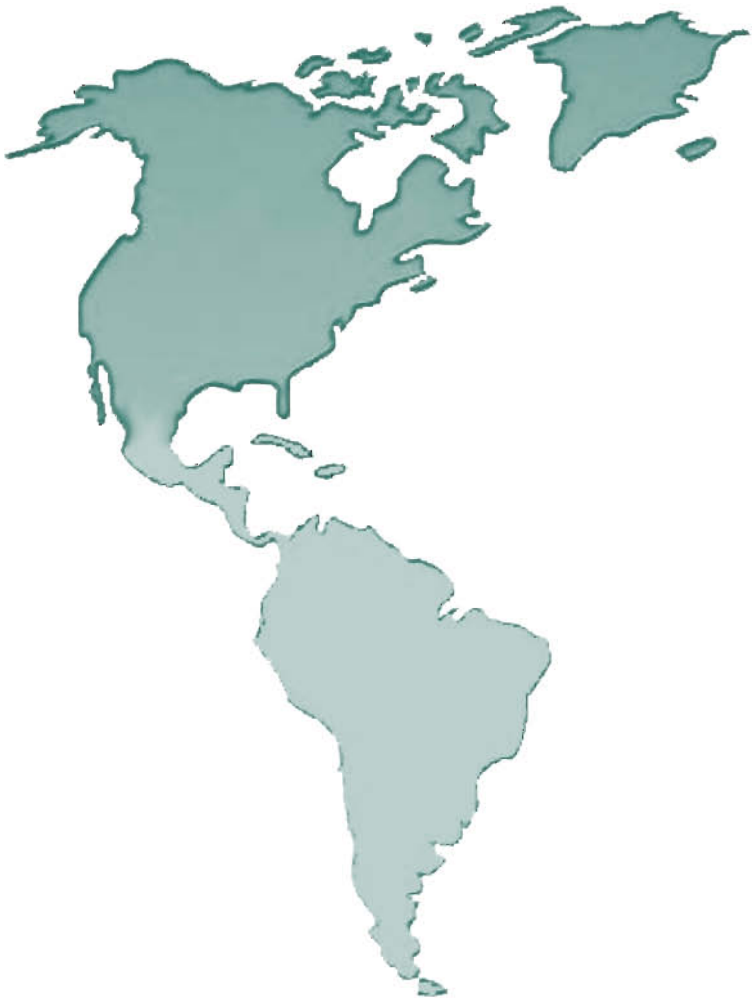
IV Encuentro Iberoamericano de Protección de Datos Personales

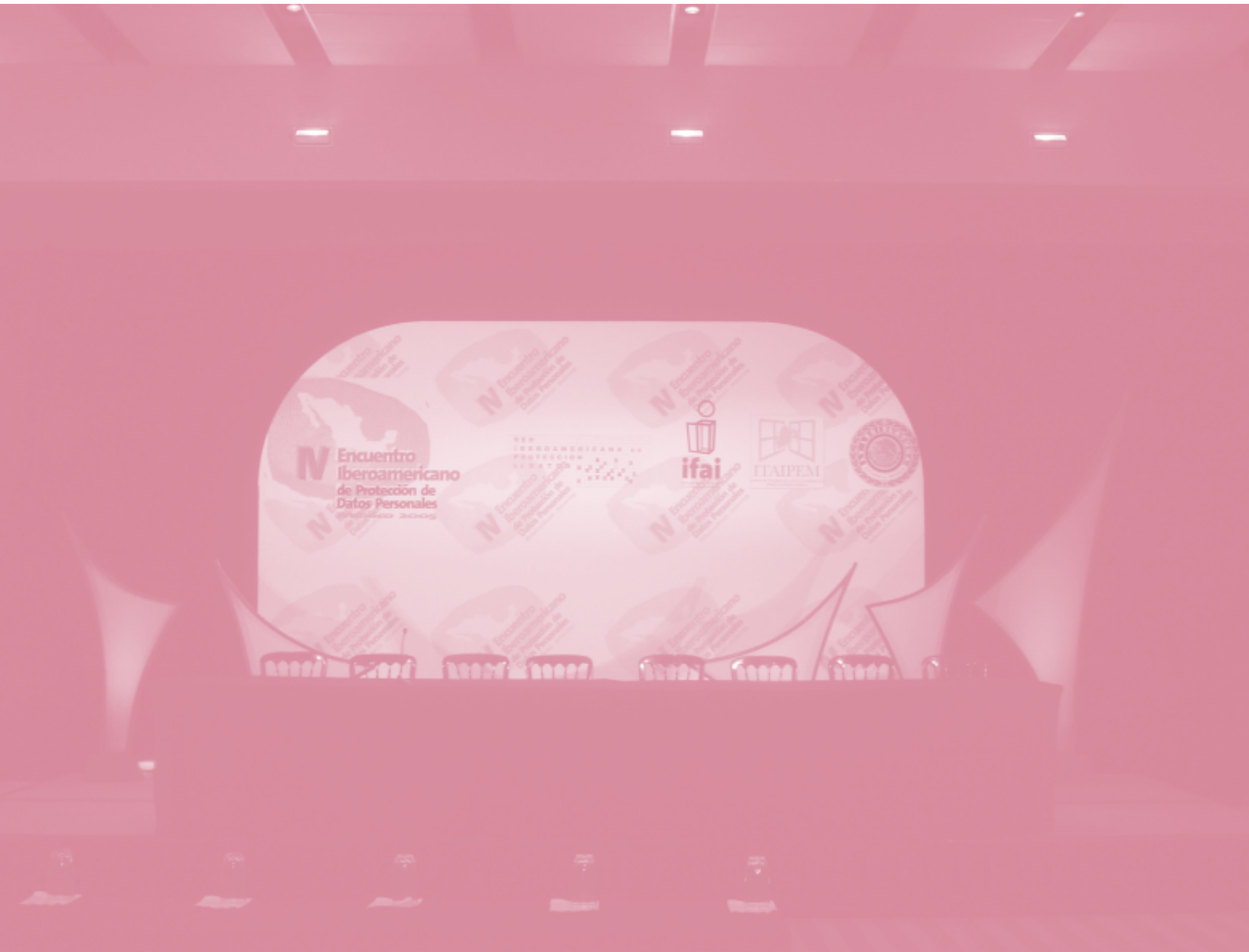
México 2005



Instituto Federal de Acceso a la Información Pública

ifai
Instituto Federal de Acceso a la Información Pública

Instituto Federal de Acceso a la Información Publica



Directorio:

Alonso Lujambio Irazábal
Comisionado Presidente

Horacio Aguilar Álvarez de Alba
Comisionado

Alonso Gómez Robledo Verduzco
Comisionado

Juan Pablo Guerrero Amparán
Comisionado

María Marván Laborde
Comisionada

Francisco Ciscomani Freaner
Secretario de Acuerdos

Ángel Trinidad Zaldívar
Secretario Ejecutivo

Instituto Federal de Acceso a la Información Pública (IFAI)
Av. México 151, Col. Del Carmen, C.P. 04100,
Delegación Coyoacán, México, D.F.
Primera Edición, IFAI
ISBN: 968-5954-32-1

Impreso en México / *Printed in Mexico*
Distribución gratuita

Índice

Mensajes en el acto inaugural IV Encuentro Iberoamericano de Protección de Datos Personales

Este evento ha sido convocado por la Red Iberoamericana de Protección de Datos Personales, y organizado por el Instituto Federal de Acceso a la Información Pública (IFAI), con la colaboración de la LV Legislatura del Estado de México y el Instituto de Transparencia de Acceso a la Información Pública del Estado de México (ITAIPEM).

La Red Iberoamericana de Protección de Datos Personales es un foro permanente de intercambio de información y experiencias abierto a todos los países miembros de la Comunidad Iberoamericana; tiene como objetivo impulsar los desarrollos necesarios para garantizar una regulación avanzada de este derecho fundamental.

Presidium:

Horacio Aguilar Álvarez de Alba. Comisionado del Instituto Federal de Acceso a la Información Pública (IFAI).

José Luis Piñar Mañas. Director de la Agencia Española de Protección de Datos y Presidente de la Red Iberoamericana de Protección de Datos Personales.

Rolando Barrera Zapata. Consejero Presidente del Instituto de Transparencia y Acceso a la Información Pública del Estado de México (ITAIPEM).

Luis Gustavo Parra Noriega. Diputado local de la LV Legislatura del Estado de México.

María Marván Laborde. Comisionada Presidenta del Instituto Federal de Acceso a la Información Pública (IFAI).

Ponente: Horacio Aguilar Álvarez de Alba. Comisionado del IFAI.

Es un significado honor para su servidor poder dar un breve mensaje de bienvenida con motivo de este IV Encuentro en materia de Protección de Datos Personales.

Me parece que aquí se encuentran varias coordenadas históricas. La primera es que es un encuentro, verdaderamente es volver a hacer contacto con la cultura iberoamericana, cultura ibérica con la americana fundidas en una sola para crear una nueva y diferente.

Esto da lugar a reflexionar sobre nuestras raíces y sobre nuestro sistema jurídico.

México ha sido un país experto en mestizajes y sobre todo, en mestizajes jurídicos. El primero se dio en la época del Virreinato, donde el sistema jurídico se integró mediante normas provenientes del Reino de Castilla debidamente adaptadas al sistema propio de nuestra comunidad. De ahí surgió una importantísima institución jurídica, que a la fecha tiene notables referencias.

Cuando alguna disposición jurídica no era susceptible de aplicarse el Virrey al recibirla decía: Obedézcase, pero no se cumpla.

Esto es de alguna manera, el origen de una buena parte de nuestra cultura donde encontramos una gran tendencia al no cumplimiento de la misma.

Pero también hay que recordar que nuestro sistema jurídico es románico, germánico, canónico, se consolida en la época del Virreinato, el derecho novo hispano o indiano sobrevive muchos años después de la Independencia.

El segundo mestizaje lo encontramos, jurídicamente hablando, en el año de 1824, cuando México llega a la independencia, quiere entrar a la modernidad, decide tener una constitución y por la influencia del embajador de los Estados Unidos de América, que fue el primero que reconoció como gobierno la independencia de nuestro país, se empieza a difundir la Constitución Americana y se copia el régimen federal.

Nuestro artículo 124 constitucional es una copia literal de la norma correlativa de la Constitución Americana.

Cuánto trabajo nos ha costado implementar el régimen federal en nuestro país; tenemos notables avances, aunque en algunas materias todavía existe el rezago.

El último mestizaje del cual estamos siendo espectadores y en muchas ocasiones hasta actores, se da por virtud de la suscripción del Tratado de Libre Comercio entre México, Estados Unidos y Canadá. México tiene esa gran capacidad de adaptación al cambio y a las normas jurídicas.

Hoy, este encuentro nos permitirá una reflexión seria y responsable sobre la cuestión relativa a la normatividad en materia de datos personales. Es importante resaltar que los datos personales son trascendentes porque son el reflejo de la persona, no son la persona misma, son el reflejo de la persona.

Y por lo tanto vamos a encontrar que en nuestro sistema jurídico mexicano hay una gran cantidad de disposiciones encaminadas a proteger los datos personales porque protegen a la persona.

Estamos en presencia de una visión personalista, desde el Derecho Constitucional, desde la Constitución misma pero, sobre todo, en nuestro Derecho Civil.

Hoy tenemos que ir avanzando en esta materia para ir haciendo reflexiones de cómo ampliar o dilatar la protección de los datos personales.

Con estas breves reflexiones que me permito extrovertir con ustedes, me permito hacer la más cordial bienvenida para todos los participantes, no solamente augurando, sino asegurando los

éxitos más acabados de esta reunión que habrán de concluir no solamente con una proclama en esta materia, sino que habrán de concluir con una fórmula que haga estable la reflexión libre en materia de derechos personales.

Ponente: José Luis Piñar Mañas. Director de la Agencia Española de Protección de Datos y Presidente de la Red Iberoamericana de Protección de Datos Personales.

Es para mí un honor y una satisfacción poderme dirigir a todos ustedes en la Ciudad de México con motivo de la celebración del IV Encuentro Iberoamericano de Protección de Datos Personales.

En esta ocasión nos reunimos representantes de 17 países, siguiendo el camino ya empezado con la *Declaración de la Antigua*, Guatemala en el año 2003. Entonces, un grupo de personas representantes de diversas instituciones decidimos crear la Red Iberoamericana de Protección de Datos.

Poco después, los jefes de Estado y de gobierno de los países de la Comunidad Iberoamericana en la *Declaración de Santa Cruz de la Sierra* hicieron mención expresa a la Red Iberoamericana de Protección de Datos e hicieron mención expresa al derecho fundamental a la protección de datos personales. La Red, por tanto, había alcanzado ya carta de naturaleza, había obtenido el más alto reconocimiento por parte y con absoluta unanimidad de todos y cada uno de los jefes de Estado y de gobierno de todos los países integrantes de la Comunidad Iberoamericana.

Tras celebrar el *III Encuentro en Cartagena de Indias*, nos encontramos celebrando este IV Encuentro, respecto del cual estoy seguro que se va a poder decir que ha habido un antes y un después del IV Encuentro Iberoamericano de Protección de Datos Personales.

Como antes se comentaba, la Red está abierta a la participación de todos y cada uno de los países miembros de la Comunidad Iberoamericana, ya contamos con representantes, como antes apuntaba, de 17 Estados miembros.

Es para nosotros, por tanto, no sólo un honor sino un acicate para seguir trabajando, para seguir colaborando entre todos para intercambiar experiencias, para colaborar en el desarrollo de procesos regulatorios con el fin de consolidar el derecho fundamental a la protección de datos personales.

Ya en Guatemala se señalaba que los integrantes de la Red constatábamos la necesidad de impulsar la adopción de medidas que garanticen un elevado nivel de protección de datos, así como la idoneidad de contar con marcos normativos nacionales que, inspirados en tradiciones jurídicas comunes en el respeto a los derechos fundamentales y en los intereses de sus respectivos países garanticen una protección adecuada en todos los países iberoamericanos.

Tales marcos normativos deberían tomar en consideración los principios esenciales de protección de datos reconocidos en los instrumentos internacionales.

En este sentido, se decía, se consideraba muy positivas las iniciativas regulatorias que se han puesto en marcha en diversos países iberoamericanos.

Se decía también que los miembros de la Red éramos conscientes de que el derecho a la protección de datos personales fortalece el Estado de derecho y ayuda a reforzar la democracia en los países iberoamericanos, así como su prestigio y credibilidad en un mundo globalizado. A tal fin se constituyó, como digo, la Red que ahora celebra este IV Encuentro Iberoamericano.

La idea es que de este Encuentro surja una declaración, la *Declaración de México* que vaya o que incluya la adopción de cuatro documentos de trabajo en los que se está trabajando ahora.

Sí que querría, antes de terminar, decirles que en la última Conferencia Mundial de Protección de Datos celebrada en Suiza, a instancias de las delegaciones francesa y española se hizo una referencia expresa en la declaración final, al reconocimiento de los esfuerzos que en los países iberoamericanos y en los países de lengua francesa se está haciendo para potenciar el derecho fundamental a la protección de datos personales.

Tal derecho puede y debe convivir con otros derechos fundamentales, cuáles son, el derecho a la libertad de expresión, el derecho a la libertad de acceso a la información, esencial en el desarrollo de las sociedades democráticas, pero no desde una perspectiva de confrontación, sino muy al contrario desde una perspectiva de complementar con ambos soportes la construcción de los Estados democráticos.

Agradezco al IFAI por el enorme esfuerzo que ha hecho para que este Encuentro sea posible y agradecer a cuantas personas, con nombres y apellidos, que ahora todos tenemos en la cabeza, han hecho posible. Por supuesto, agradecer también la colaboración de la Quincuagésima Quinta Legislativa del Estado de México, así como del Instituto de Transparencia y Acceso a la Información Pública del Estado de México, ITAIPEM.

Ponente: Rolando Barrera Zapata. Consejero Presidente del Instituto de Transparencia y Acceso a la Información Pública del Estado de México, ITAIPEM.

Para el Instituto de Transparencia y Acceso a la Información Pública del Estado de México, resulta significativo y alentador participar como copatrocinador, junto con el IFAI, la Legislatura del Estado de México y la Red Iberoamericana de Protección de Datos Personales, de este trascendente IV Encuentro Iberoamericano.

Es significativo, en razón de que hoy, en nuestro país, la necesidad de legislar para proteger la información concerniente a las personas, forma parte ya de la agenda institucional de los gobiernos.

La precisión de los alcances, mecanismos e instancias que garanticen la protección de datos personales, serán cuestiones, entre otras, que se atendrán con la intervención, sin duda, de las distintas comisiones, órganos e institutos que tienen ya este cometido dentro de sus deberes institucionales.

Es alentador porque el ITAIPEM, así lo consideramos, forma parte ya de esta importante Comunidad Iberoamericana, que ha venido trabajando de tiempo atrás en esta materia, cuyo contenido cobra mayor relevancia ante los constantes progresos de las telecomunicaciones, la informática y la telemática.

En el ITAIPEM defendemos la convicción institucional de que el derecho de acceso a la información tiene como complemento el derecho a la protección de datos personales, en tanto la garantía que tiene el particular de poder controlar sus datos personales y manifestar su consentimiento, respecto del uso o tratamiento que se le den a sus propios datos.

El ITAIPEM está comprometido con la salvaguarda del sano equilibrio entre el acceso a la información pública y la protección de datos personales, no sólo porque así se lo impone la legislación que lo rige, sino porque este equilibrio es pertinente para el respeto de la privacidad e intimidad de todos, incluyendo lo que corresponda a la de los propios servidores públicos.

Estamos ciertos de que este IV Encuentro Iberoamericano de Protección de Datos Personales logrará plenamente sus objetivos y nos congratulamos de que hayan ustedes aceptado nuestra anfitrionía para el día viernes 4 de noviembre, en la sede de la Universidad Anáhuac, en el Municipio de Huixquilucan, Estado de México.

Ponente: Luis Gustavo Parra Noriega. Diputado local de la LV Legislatura del Estado de México.

A nombre de la LV Legislatura del Estado de México les doy la más cordial bienvenida a este IV Encuentro Iberoamericano de Datos Personales, esperando que estos tres días sean de un fructífero trabajo y de una discusión amplia y de mucha riqueza.

La definición de democracia de Robert Dall, sugiere que dicho régimen cuente con una serie de principios mínimos, tales como, sufragio universal, elecciones regulares, libres, competitivas y justas, más de un partido político, más de una fuente de información, además de contar con instituciones democráticas, derechos existentes y procesos de toma de decisión que no estén restringidos por una élite.

Asimismo, una buena democracia o democracia con calidad, como lo define Leonardo Morlino, se caracteriza por ser un régimen ampliamente legitimado, que satisface completamente a los ciudadanos en la que estas asociaciones y comunidades que la componen disfrutan de libertad de igualdad y donde los propios ciudadanos pueden verificar y evaluar si el gobierno trabaja por los objetivos precisamente de libertad e igualdad.

La libertad, la igualdad y la rendición de cuentas son los presupuestos fundamentales para establecer y llevar a cabo políticas gubernamentales y políticas democráticas de calidad.

Los principales temas de una democracia de calidad, según Morlino, son los ciudadanos individuos, las comunidades territoriales y las diversas formas de asociación con valores, tradiciones o fines comunes, temas que por lo demás están adquiriendo un lugar preponderante en la agenda política de nuestro país y que impactan los procesos de toma de decisión.

Con el cambio político que experimentó México a partir del año 2000 hemos iniciado un proceso inédito para seguir construyendo el país que queremos y consolidar un sistema democrático que además de garantizar reglas claras y confiables para la competencia electoral y el acceso al poder, asegure el ejercicio transparente de la función pública, de tal modo que la sociedad pueda conocer y evaluar la gestión gubernamental y el desempeño de los servidores públicos.

Ello implica recuperar para la nación y para los ciudadanos el espacio público, generando las condiciones necesarias para que la sociedad pueda desarrollar todas sus capacidades en un contexto de libertad y de responsabilidad social.

En este sentido, un logro del actual gobierno federal se ha manifestado con el reconocimiento de un derecho fundamental, necesario para el funcionamiento de las democracias modernas que fomente una relación distinta entre la sociedad y el Estado, es decir, el acceso a la información pública. Este derecho inherente de cualquier democracia moderna se concretó en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, divulgado el pasado 11 de junio del año 2002, retomando principios de diversos instrumentos del derecho internacional, en donde se reconoce la libertad de toda persona de buscar, recibir y difundir información de toda índole sin consideraciones de fronteras, ya sea oralmente o por escrito, en forma impresa o por cualquier otro procedimiento.

Actualmente sólo cuatro estados de la República no han expedido leyes de transparencia y acceso a la información, lo cual resulta un grave avance en la implementación de este derecho.

Es innegable que las políticas de transparencia ayudan a eliminar o al menos a reducir las asimetrías de información entre las organizaciones gubernamentales y la sociedad; por lo tanto, es de esperarse que la relación Estado-sociedad se fundamente en el desempeño del gobierno como administrador de los recursos públicos de una manera abierta y accesible.

Por otra parte, la globalización es una realidad, es un fenómeno multidimensional que abarca no sólo aspectos económicos, sino también, sociales, ideológicos, políticos, culturales, etc.; y es que las nuevas tecnologías de la información, el desarrollo de las telecomunicaciones ponen a disposición del usuario todo tipo de información incluida información personal, que es claramente utilizada para fines comerciales y de mercadotecnia, pero la mayoría de las veces estos datos pueden ser manipulados sin el consentimiento del titular y peor aún si se tiene un total desconocimiento de su tratamiento, uso y destino de dichos datos.

Y ante esta situación la persona queda en estado de total indefensión sin encontrar los mecanismos para acceder a sus datos, solicitar que sea retirada de esas listas de destinatarios o reclamar sobre actos de discriminación derivados del conocimiento por parte de terceros de sus datos personales.

En la mayor parte de los países de América Latina no se ha generado un debate amplio y adecuado sobre los alcances del intercambio generalizado de información, a fin de garantizar un marco de libre flujo de la información, y menos aún para proteger la intimidad o privacidad de las personas.

Considero de vital importancia que los gobiernos tomen las medidas correspondientes para regular este aspecto, más allá de los beneficos comerciales que representa o por cumplir con tratados internacionales suscritos, sino más bien con el convencimiento que está legislando a favor del ciudadano.

Encuentro también que el principal desafío de las democracias de América Latina, y particularmente en México es, por un lado, garantizar el acceso a la población a todas las fuentes de información disponibles, y las nuevas tecnologías; pero también, por otro lado, garantizar el respecto de los derechos humanos fundamentales, específicamente los derechos que tienen que ver con estas materias.

Afortunadamente en muchos países en diversas partes del mundo han preparado el terreno en la materia, y tenemos a la mano diversas fuentes enriquecedoras para aquellos países en los que aún nos falta camino por recorrer.

Es primordial entonces dejar muy claro que los datos personales son un derecho fundamental que debe permitir a la persona tener el control sobre su uso, su tratamiento, su destino y su acceso en el momento que lo requiera.

En otras palabras darle a la persona el poder de disposición sobre sus datos personales.

Es por ello que celebro la realización de este IV Encuentro Iberoamericano de Protección de Datos Personales, y me congratulo por el hecho de que no solamente a nivel federal, sino también concretamente el Estado de México, entidad que en este momento me toca representar a nombre de la LV Legislatura, sean los foros en donde se discuta, debata y propongan ideas sobre el tema, y especialmente se dé a conocer la trascendencia de este derecho, no solamente para los tomadores de decisiones, sino a la sociedad, que es la principal destinataria de dichos beneficios y cuyos derechos deben ser siempre respetados.

En ese sentido estoy convencido que los principales actores políticos y económicos deben centrar su acción en la primacía de la persona humana, protagonista principal y destinatario definitivo de la acción política, y buscar que el ejercicio responsable de la libertad en la democracia conduzca a la justicia y a la libertad, así mismo a la igualdad de oportunidades para la consecución del bien común.

Toda forma de discriminación y desigualdad de oportunidades por razones de sexo, edad, capacidad física, etnia, religión, convicción, condición económica o cualquier otra, debe ser rechazada, corregida y en su caso sancionada.

Por su carácter de persona el ser humano es sujeto de derechos y obligaciones fundamentales. El respeto a estos derechos y el

cumplimiento de estas obligaciones no son sólo el cimiento de toda convivencia democrática, sino la base de cualquier sociedad justa y de la paz en general.

Estoy seguro que los trabajos que se realizarán en este IV Encuentro van a enriquecer el debate en nuestro país y en toda Iberoamérica y sin duda, van a contribuir a revalorizar el papel de la persona frente a los desafíos de la globalización, de las decisiones políticas, de los flujos comerciales; pero también, van a fortalecer el proceso democrático en la región, permitiendo construir democracias con calidad que satisfagan las necesidades de los ciudadanos.

Declaratoria inaugural de los trabajos del IV Encuentro Iberoamericano de Protección de Datos Personales

Ponente: María Marván Laborde. Comisionada Presidenta del Instituto Federal de Acceso a la Información Pública (IFAI).

Antes me permitiré dar un breve mensaje:

No hay plazo que no se cumpla y hoy comenzamos el IV Encuentro de la Red Iberoamericana de Protección de Datos Personales, reciban ustedes un caluroso saludo de bienvenida.

El IFAI los recibe con los brazos abiertos. La Ciudad de México, el Estado de México, serán recintos de este encuentro, trascendente sin duda para el país y la región.

Tengo el agrado de dar este mensaje de inauguración del IV Encuentro Iberoamericano de Protección de Datos Personales, al lado de los señores José Luis Piñar Mañas, Director de la Agencia Española de Protección de Datos y Presidente de la Red Iberoamericana de Protección de Datos Personales; Rolando Barrera Zapata, Presidente del Instituto de Transparencia y Acceso a la Información Pública del Estado de México; Luis Gustavo Parra Noriega, Diputado de la LV Legislatura del Estado de México, así como de mi estimado colega Horacio Aguilar Álvarez de Alba, Comisionado del IFAI. Saludo, también, la presencia de los Comisionados del IFAI, así como del ITAIPEM y a todos ustedes.

No tengo duda de la relevancia que tiene un evento internacional, en el que se discuten los principios fundamentales para la protección de datos personales, porque parto de la premisa de que una sociedad democrática y justa supone tanto la transparencia del gobierno y la existencia de una cultura política participativa, así como la protección de la persona y de la vida privada y la intimidad.

Es innegable que el respeto a la dignidad de la persona es un valor central de todo Estado democrático, que tiene como fundamento la búsqueda de la justicia, la libertad, la igualdad, la seguridad y la solidaridad.

A partir de la afirmación de nuestra dignidad humana, se legitiman todos nuestros derechos y se hace posible ejercerlos a plenitud.

Entendemos que la democracia está ligada a la vigencia y la promoción de los derechos humanos. Pero un Estado que se asuma democrático tiene la encomienda de ir más allá de asegurar la existencia de un catálogo de libertades.

Se trata de crear y poner en marcha mecanismos de protección, que garanticen su pleno ejercicio. No podemos hablar de privacidad sin establecer una normatividad práctica que se haga cargo de la protección de las personas en relación al tratamiento de sus datos.

Contamos con un derecho fundamental a la privacidad que para que sea plenamente ejercido y garantizado debe ser reconocido por el Estado.

En la Constitución Política de los Estados Unidos Mexicanos se establece el derecho a la vida privada, como límite a la intromisión del Estado en el ámbito de la persona.

El artículo 16 de la Carta Magna es elocuente: *Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.*

En nuestro ordenamiento legal, es imprescindible el diseño de una Ley de Protección de los Datos Personales. Este tipo de leyes tocan la esencia misma de la democracia y su complejidad deriva de la demanda filosófica y jurídica de lograr establecer un equilibrio justo entre los intereses individuales, las necesidades del Estado y las demandas, cada vez más acuciantes, de un mercado que aparece en eterna expansión.

Trazar líneas que definan claramente entre lo público y lo privado, es un reto jurídico que debe acometerse con la mayor responsabilidad.

Los avances tecnológicos plantean nuevos retos, la cibernética y las telecomunicaciones, así como los avances en investigaciones genéticas obligan a planteamientos más complejos y demandan la integración de la ética social y política como eje articulador de esta discusión.

El respeto por los derechos humanos adquiere una nueva dimensión en la era de la información.

La complejidad de la vida moderna nos plantea un hombre multifacético, que debe ser protegido en muy distintos ámbitos y de diferentes maneras.

Una ley de esta naturaleza deberá hacerse cargo de proteger al individuo en su dimensión de consumidor y, al mismo tiempo, proteger el mercado, a fin de asegurar una economía que pueda objetivamente basarse en la confianza documentada.

No podemos soslayar que los datos personales también incluyen aquellos contenidos en los expedientes médicos. Éstos son, entre otros, datos sensibles cuya publicidad afecta de manera más profunda la intimidad de una persona.

Es por ello necesario distinguir conceptual y normativamente que la naturaleza de los datos puede ser diversa y, por tanto, su recolección, tratamiento y transmisión suponen medidas acordes al impacto que puede llegar a tener su difusión o el mal uso de los mismos. He ahí el reto del legislador.

Aunque actualmente mucha de esta información ya está almacenada, sistematizada y, de hecho, circula al margen de nuestro control, el objetivo de una ley de datos personales consiste en reglamentar, sin entorpecer, las formas de circulación, garantizando siempre y por encima de todo el derecho a la privacidad de los individuos.

La tecnología moderna plantea retos nada sencillos, la capacidad de acumular información parece ser infinita. En términos materiales los archivos han dejado, prácticamente, de ocupar espacio físico y la posibilidad de su transmisión en cuestión de segundos a cualquier rincón del planeta al que llegue Internet, es una realidad que demanda ser reconocida por esta legislación.

Es primordial que estas reglas sean claras y sencillas para que fomenten la circulación y exijan el adecuado tratamiento de los datos por

parte de las entidades públicas y privadas. Su fin último es fomentar la confianza de los ciudadanos, del Estado y de la esfera de la economía, siempre en el marco de los derechos humanos.

El objeto de la ley es la regulación del derecho a la autodeterminación informativa de las personas. Su ámbito de aplicación de ésta reside en las bases de datos, estén o no automatizadas. Por lo tanto, el legislador debe estar consciente de las distintas lógicas que imperan en la creación y manejo de las mismas, tanto en el sector privado como en el público.

Es difícil, si acaso imposible, imaginar una sola justificación ética para que el Estado venda a la iniciativa privada o al propio gobierno las bases de datos personales, para que sean utilizadas con fines distintos a aquéllos para los que fueron proporcionados por el individuo, quien es el propietario único y el beneficiario directo de esta información. Al comprometerse a proteger la privacidad, el Estado defiende la autonomía de los individuos como condición básica del orden social.

En nuestro país no contamos aún con un marco normativo comprensivo, que considere tanto al sector público como al privado en su conjunto, sobre la protección de los datos personales.

Será necesariamente una decisión del Congreso de la Unión la determinación del diseño legal, así como el entramado institucional que conduzcan hacia la correcta operación y vigilancia de las disposiciones jurídicas que habrán de configurar la política de Estado, para la protección de los datos personales.

Quiero hacer un reconocimiento público a la labor del senador Antonio García Torres, quien ha sido uno de los principales promotores de esta ley y ha logrado poner el tema en la agenda nacional.

Sin lugar a dudas, la democracia en México será cualitativamente más sólida en la medida en que garantice efectivamente la protección a la privacidad.

El IFAI, como autoridad garante de la protección de las personas respecto del tratamiento de sus datos en el ámbito de la Administración Pública Federal, ha estado atento al desarrollo de los trabajos parlamentarios para la aprobación de una ley de datos personales; hemos trabajado tanto con el Senado, así como con la Cámara de Diputados porque nos preocupa concretar la normatividad y asegurar que avance el tema en beneficio de todos los ciudadanos.

Para ello es indispensable incorporar a la discusión la complejidad íntegra del debate. Sería un grave error lograr avances en la custodia de los expedientes médicos sin la integración de la perspectiva financiera. Igualmente desastroso sería reducir la dimensión de la privacidad a la visión mercantilista que reduce al ser humano como consumidor.

Asumimos, como nuestra responsabilidad de cooperar en el ámbito de nuestras competencias y posibilidades con el Legislativo, para la aprobación de una buena ley, y para ello, ponemos al servicio de la sociedad tanto nuestros recursos humanos y materiales como la experiencia adquirida en estos tres años, en que la sociedad y el legislador nos han confiado la protección de los datos personales en manos de la Administración Pública Federal.

Hemos tenido la oportunidad de dimensionar tanto la delicadeza del tema como su complejidad y, sabemos por experiencia, que es indispensable avanzar con pasos firmes y aprender de la práctica internacional.

Desde el año 2002 la Red Iberoamericana de Protección de Datos en colaboración con la Agencia Española de Protección de Datos, han organizado este Encuentro.

Este año, representantes de 17 países de la Comunidad Iberoamericana participarán en un foro de intercambio de información y debate

sobre asuntos de la mayor actualidad y trascendencia en materia de protección de datos, que permita la cooperación mutua y la promoción del derecho a la privacidad en el entorno iberoamericano.

Algunos países ya han aprobado y aplicado estas leyes; podremos abrevar de su experiencia. Reconocemos que hay mucho por hacer y que la novedad del tema nos obliga a plantear dilemas específicos y experiencias jurídicas complicadas que habremos de enfrentar en la discusión colegiada entre países hermanos.

Con la participación de todos ustedes se favorecerán los intercambios de ideas y vivencias entre las autoridades de protección de datos, representantes de organizaciones provenientes de los sectores público y privado, así como académicos y organismos internacionales, con temas tales como el impacto de las tecnologías de la información, el Internet y las telecomunicaciones sobre la privacidad, la protección de los datos en el sector financiero y comercial, las iniciativas de leyes de protección de datos personales en el ámbito federal y en los estados de la República, las medidas de seguridad para la protección de la información, sin denostar, desde luego, el debate de ideas y experiencias en torno al derecho fundamental del derecho a la privacidad.

Reitero que sin una protección adecuada de los datos personales, todos nosotros perdemos un derecho fundamental. La privacidad va de la mano de la libertad. Ambas son condiciones para la democracia.

Del pleno ejercicio de este derecho, así como del adecuado diseño legal e institucional para la protección de los datos personales, depende de cada uno de nosotros, desde nuestras respectivas esferas de acción.

No me queda sino agradecer a todos aquellos que con su tenacidad y empeño, han hecho posible que hoy estemos aquí todos reunidos. La persistencia de la propia Red así como de la Agencia Española, ha sido crucial para ello. Agradezco también al Instituto de Transparencia y Acceso a la Información del Estado de México, así como al Congreso de la entidad.

Por último, pero no por ello menos importante, al personal del IFAI que no ha escatimado en esfuerzos, y de manera muy especial, a la Dirección de Clasificación y Datos Personales, así como al comité organizador de este evento. Sin sus desvelos y preocupaciones esto no habría sido posible.

No puedo dejar de mencionar al Comisionado Aguilar Álvarez coordinador de estos esfuerzos.

Sin más por el momento, damos inicio a este IV Encuentro Iberoamericano de Protección de Datos Personales.

Confío en que todas las ideas, experiencias y diálogos que tengan lugar en cada una de las mesas, sean del máximo provecho para todos nosotros.

Si se ponen de pie para la declaración de inauguración.

Siendo las 10 de la mañana del día 2 de noviembre en la Ciudad de México, declaro formalmente inaugurados los trabajos de este IV Encuentro Iberoamericano de Protección de Datos Personales, México 2005.

El derecho fundamental a la protección de los datos personales

Mesa 1

Moderador: Fernando Corvera Caraza. Director de disposiciones de *Banca Central* del Banco de México.

La Conferencia Magistral esta a cargo de José Luis Piñar Mañas, quien es Director de la Agencia Española de Protección de Datos y Presidente de la Red Iberoamericana de Protección de Datos Personales; Vicepresidente del Grupo Europeo de Autoridades de Control de Protección de Datos Personales; doctor en Derecho por la Universidad Complutense, catedrático de Derecho Administrativo, ha sido decano en las facultades de Derecho de las universidades de Castilla, Mancha y San Pablo en Madrid; ha sido premiado en la Real Academia Española de Jurisprudencia y Legislación y ha tenido el premio de investigación de la Conferencia Iberoamericana de Fundaciones.

Conferencia Magistral: José Luis Piñar Mañas.

Muchas gracias a los organizadores por darme la ocasión de exponerles algunas reflexiones acerca del derecho fundamental a la protección de datos personales.

Antes les quería comentar algunos datos sumamente importantes que seguramente nos impactarán. El pasado 27 de enero de este año se conoció que mediante decisión de diciembre del año 2004 el Tribunal Federal de Suiza acordó seguir adelante con la reclamación presentada por un grupo internacional de personas de raza gitana, contra una multinacional de las telecomunicaciones, una multinacional que había posiblemente colaborado con los nazis, que habrían utilizando su tecnología de tarjetas perforadas para la identificación y exterminio de judíos y gitanos.

En 2001 fue publicado un impresionante libro de Edwin Black, *IBM y el Holocausto*, en el que denuncia que el uso de las máquinas tabuladoras y tarjetas perforadas por la empresa filial –Dehomag– de esa multinacional en Alemania fue decisivo para elaborar el censo alemán de 1937 e investigar los antecedentes raciales de toda la población alemana, lo que habría facilitado decisivamente la identificación y localización de los judíos cuya dirección se incluía en cada ficha.

Este fue el origen del Holocausto, y por eso se pudo ir en un primer momento directamente a las casas, a los domicilios de las personas de raza gitana, a las personas de la comunidad judía.

La multinacional –IBM–, además de condenar tajantemente el régimen nazi niega totalmente su participación, y afirma que con la llegada al poder de Hitler perdió todo el control sobre su filial –Dehomag–.

Allá por los años cincuenta ó sesenta una muy importante empresa italiana, FIAT, recogió en una base de datos, todos los datos posibles acerca de todos sus trabajadores relacionados no sólo con los datos necesarios para llevar el control, la gestión de personal de la empresa, sino también incorporando datos de religión, de afiliación sindical, de afiliación política. Lo cual permitió llevar a cabo diversas actuaciones de la empresa contra algunos de los trabajadores.

Hoy se considera que se envían diariamente en todo el mundo decenas de miles de millones de correos electrónicos no deseados. Más del 80 por ciento de los correos electrónicos son ilegales. La invasión de la intimidad o los daños que derivan de los virus, además del trastorno y pérdida de tiempo que se ocasiona a los usuarios son ya enormemente graves.

Mediante los llamados identificadores de radiofrecuencia, RFID, es posible localizar no sólo productos, sino también personas, sin que éstas sean conscientes de ello. El mal uso de datos genéticos puede condicionar, cuando no bloquear, la suscripción de una póliza de seguros o una contratación laboral.

Nunca antes ha sido posible saber tanto de tantas personas.

La obra *1984*, es común citar esta obra de George Orwell, es posible *Minority Report*, *Inteligencia Artificial* es posible. No son ciencia ficción, son realidad.

Hoy, como digo, es posible saber mucho de mucha gente y saberlo sin que esa propia gente sea consciente de que alguien sabe de su vida, incluso, más que la propia persona.

Es por ello por lo que es absolutamente imprescindible el contar con un marco regular que respete, que reconozca, que regule el derecho fundamental a la protección de datos personales.

Un derecho que forma parte intrínseca de la propia dignidad de la persona, porque en definitiva cuando se trata de nuestros datos personales, cuando trata alguien nuestros datos personales está jugando con nuestra identidad, está jugando con la dignidad de las personas.

Voy a referirme brevemente al origen de la regulación sobre protección de datos personales, para analizar cómo hemos llegado en estos momentos al reconocimiento de un verdadero derecho fundamental.

En 1888, en el siglo XIX, Thomas McIntyre Cooley habló ya de the right to be let alone, el derecho a ser dejado en paz y poder disfrutar libremente de la privacidad o el derecho a la soledad.

En el volumen 4 del 15 de diciembre de 1890, todos ustedes saben, Samuel Warren y Luis Brandeis, publican en Harvard Law Review, su famoso artículo *The Right to Privacy*, a quien no hace mucho se refería el que ha sido hasta hace poco presidente del grupo de autoridades de protección de datos personal, Stefano Rodotá. En aquel entonces los autores hablaban de un nuevo derecho. Decían: *Los cambios políticos, sociales y económicos implican el reconocimiento de nuevos derechos y el Common law, dice en su eterna juventud alcanza a atender las nuevas demandas de la sociedad*.

Ahora el derecho a la vida se ha convertido en el derecho a poder vivir, a poder disfrutar de la vida de '*Joe life'.* Y decían: Hay un nuevo derecho, el derecho a poder vivir solo. A que le dejen a uno solo en su vida.

Por cierto, decía Greta Garbo muy agudamente, que ella lo que quería no era vivir sola, sino que la dejasen vivir sola.

Este es uno de los contenidos esenciales del derecho fundamental a la protección de datos

en sus orígenes. El construir una esfera de intimidad, que les permita a las personas ser dueños de su propia privacidad, pero fíjense que en los primeros momentos de creación de generación de este derecho, el punto esencial se pone en la privacidad.

Cuando en los años sesenta se ponen en marcha los primeros mecanismos normativos para regular el derecho a la privacidad, el gran debate, la gran preocupación del legislador de entonces es conseguir que la tecnología, que la informática no supusiese una violación de la privacidad.

Ya en 1967 se constituyó, en el seno del Consejo de Europa, una comisión consultiva para estudiar las tecnologías de la información y su potencial agresividad hacia los derechos de las personas, especialmente en relación con su derecho a no sufrir injerencias en la vida privada, derecho que se había ya recogido en la Declaración Universal de Derechos Humanos o en el Pacto Internacional de Derechos Civiles y Políticos del año 1966.

De tal comisión consultiva surge la Resolución 506 de la Asamblea del Consejo de Europa, sobre los derechos humanos y los nuevos logros científicos y técnicos, que respondía a una inquietud existente en todo el Continente.

Suele decirse, no sin razón, que en tal resolución se encuentra el verdadero origen del movimiento legislativo que desde entonces recorrerá Europa y el mundo entero, en materia de protección de datos.

Es lugar común también citar la conocidísima Ley *Land* de *Jesse*, pionera en la materia, la Ley Federal Alemana del año 77, la Ley Francesa en Informática *Ficheros y Libertades* de 1978, sustancialmente modificado, por cierto, al objeto de adaptarla a la Directiva 95 96 en el año 2004.

En 1977 el Parlamento Europeo aprueba una Resolución sobre la tutela de los derechos del individuo frente al creciente progreso técnico en el sector de la informática.

En junio del 78 se aprobaron unas leyes en Dinamarca. Durante estos años, finales de los setenta, se aprueba una serie de normas que tienen, como digo, como punto de encuentro, punto común, el intentar, mediante un claro marco normativo, proteger a los ciudadanos frente al uso de la informática.

La gran tensión, los dos conceptos que están enfrentados son, privacidad, por un lado; informática por otro.

En los años ochenta, desde el Consejo de Europa se da un respaldo definitivo a la protección de la intimidad frente a la informática, mediante el conocidísimo Convenio 108 para la Protección de las Personas, con respecto al tratamiento autorizado de los datos de carácter personal.

Intenta conciliar el Convenio 108 el derecho al respeto a la vida privada de las personas con la libertad de información, facilitando la cooperación internacional, en el ámbito de la protección de datos y limitando los riesgos de desviaciones en las legislaciones nacionales.

En fin, la OCDE también publica dos importantes recomendaciones: La recomendación sobre circulación internacional de datos personal para la protección de la intimidad y la relativa a la seguridad de los sistemas de información.

En 1976 la Constitución portuguesa reconoce el derecho a la protección de datos, en el artículo 35, que se modifica en el año de 1997.

La perspectiva, como digo y reitero, es la de informática *versus* intimidad. Esta es también, por ejemplo, la perspectiva de la Constitución española de 1978, en su artículo 18.4.

Tras esta primera fase en que, como digo, se tiene en cuenta este par de conceptos, informática *versus* privacidad, en los años noventa se da un paso sustancial. Hay algo nuevo que aparece en el escenario de la protección de datos; se incorpora un elemento esencial al debate.

Se incorpora desde la construcción europea. La construcción europea requiere, en efecto, requiere ineludiblemente la construcción del mercado interior y exige que se garantice la libre circulación de los datos personales, dado el valor económico que los mismos tienen en las transacciones comerciales. Este es también un elemento capital. Hoy es imprescindible contar con datos personales, en el sector público y en el sector privado.

Desde la perspectiva de la Unión Europea, era imprescindible que la construcción del mercado interior pasase por el reconocimiento de la libre circulación de los datos personales, pero, y este es el elemento capital, con absoluto respeto a los derechos fundamentales y en particular al derecho fundamental a la protección de datos personales.

En este escenario se mueve la Directiva 95 46 del 24 de octubre de 1995. Ya sólo el título, el enunciado lo dice todo, Directiva Relativa a la Protección de las Personas Físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Al par de conceptos, por tanto, intimidad *versus* informática se añade ahora un elemento más: el valor económico de los datos personales; valor económico que debe reconocerse sin perjuicio, como digo, del respeto a los derechos fundamentales y, en particular, el respeto a la intimidad.

La construcción europea pasa por la creación del mercado interior en el respeto a los derechos fundamentales y en este marco, la libre circulación de los datos con respeto al derecho a la intimidad se considera de primerísima importancia. A este fin responde la Directiva 95 46.

Durante los años noventa se produce, además, un importante movimiento regulatorio, no sólo en Europa si no en muchos países; en España mismo se aprueba la primera Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, sólo referida al tratamiento automatizado de datos personales en el año noventa y dos.

En el año noventa y nueve se aprueba la Ley Orgánica de Protección de Datos, ya referente a todo tipo de tratamiento de datos, automatizado o no automatizado.

En los años noventa se aprueba también la Constitución de Brasil y la ley brasileña del año noventa y siete de reconocimiento de Data.

En el año noventa y nueve en la Constitución venezolana se reconocen los derechos de acceso, rectificación y cancelación a los datos personales. En el mismo año se aprueba la ley chilena de protección de la vida privada.

En el noventa y ocho la Constitución de Ecuador reconoce los derechos de acceso, rectificación y cancelación.

En el noventa y tres la Constitución de Perú reconoce el derecho de acceso a la información y el derecho a la intimidad.

En el año 2000 esta situación experimenta un giro "copernicano", tanto en la Unión Europea como en otros países, en particular en España y en otros de la Comunidad Iberoamericana.

¿Qué es lo que ocurre entonces? Surge un derecho fundamental nuevo o mejor dicho, se reconoce expresamente la existencia de un derecho fundamental nuevo, autónomo, que es capaz de emanciparse de la intimidad, de la privacidad y de la informática, es el derecho autónomo, independiente, nuevo a la protección de datos personales.

Es, en este punto esencial la Carta de Derechos Fundamentales de la Unión Europea, como saben ustedes, proclamada en Niza el 7 de diciembre del año 2000, que de forma sumamente lacónica, pero tan lacónica como de forma tajante, dispone en su artículo 8 dentro del capítulo relativo a las libertades que nada

más y nada menos toda persona tiene derecho a la protección de los datos de carácter personal que la conciernen.

No hay ninguna referencia ya a la intimidad. No hay ninguna referencia a la privacidad, no hay ninguna referencia a la informática, repito, lo que dice el artículo es: *toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan*. Por cierto, añade también, *que el respeto de estas normas sobre protección de datos, quedará sujeto al control de una autoridad independiente*.

Además, es importante resaltar que en el artículo 7 de la propia Carta, de forma separada, se recoge el derecho a la vida privada y familiar, con lo cual el redactor de la carta europea ha querido perfectamente distinguir entre el derecho a la intimidad, el derecho a la privacidad y el derecho a la protección de datos personales como dos derechos íntimamente relacionados, pero separados, diferenciados.

En España el cambio se produce de la mano del Tribunal Constitucional. El Tribunal Constitucional español dicta dos importantes sentencias, ambas del 30 de noviembre del año 2000, las sentencias número 290 y 292 que vienen a culminar un proceso jurisprudencial que se inicia en el año ya incluso 84 y que a través de diversas sentencias de los años 93, 94, 98. Culmina en 99, como digo, con la declaración de que el derecho a la protección de datos es un derecho fundamental autónomo.

Lo importante es definir este derecho y el Tribunal Constitucional español lo define como: derecho que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporcionar a un tercero, sea el Estado o un particular o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control, dice el Tribunal, sobre los datos personales que constituye parte del contenido del derecho fundamental a la protección de datos se encuentran jurídicamente en la facultad de consentir la recogida, principio de consentimientos sobre el que luego algo diré; consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero sea el Estado o un partido.

No es necesario resaltar la importancia de las construcciones jurisprudenciales y normativas a la que me estoy refiriendo.

En Argentina también en el año 2000 se aprueba la ley 25 326 de Protección de Datos. Estamos, por tanto, en presencia de un cambio radical, sustancial, como antes decía, un verdadero giro "copernicano" a favor de un nuevo derecho fundamental.

¿Cuál es entonces el problema al que ahora tenemos que enfrentarnos? Nada más y nada menos que el de definir el contenido esencial de ese derecho. Definir los principios y caracteres que lo definen y que no pueden ser desconocidos, so pena de desconocer y en consecuencia violentar el propio derecho.

En la Conferencia Internacional de Autoridades de Protección de Datos, a la que me refería antes, desde la mesa del presidium, celebrada en Montreux, Suiza, los días 13 al 15 de septiembre de 2005, se aprobó una declaración final sobre la protección de datos personales y la privacidad en un mundo globalizado.

Y se decía: un derecho universal respetando con respecto a las diversidades; se quería llamar la atención, se llama la atención acerca de la importancia de reconocer el carácter universal del derecho fundamental a la protección de datos, sin perjuicio de las diversidades propias de cada realidad cultural, política y social.

Pero en esa declaración final se adelantaban, se recogían una serie de principios esenciales del derecho fundamental a la protección de datos.

En mi opinión los principios de tal derecho, los más nucleares de la configuración del derecho pueden reconducirse a los siguientes: consentimiento, información, finalidad, calidad de los datos con especial referencia a la proporcionalidad, seguridad y el que yo podría o el que yo denominaría quizá el principio del control independiente.

Estos principios son, como digo, los que configuran el derecho fundamental a la protección de datos. Antes de decir dos palabras sobre tales principios, sí que querría resaltar el marco en el que se mueve el derecho a la protección del derecho. Al objeto de distinguirlo de otros derechos distintos o diferentes. Nos estamos refiriendo a datos personales, cualquier tipo de dato personal, no sólo los datos íntimos, no sólo los datos que afecten a la privacidad, sino cualquier tipo de dato personal, el contenido del derecho implica que cada ciudadano es dueño de sus datos personales, sean éstos o no íntimos, por tanto hablamos de datos personales, y hablamos de datos personales que estén sometidos a tratamiento informatizado o no informatizado, para decirlo más simplemente que estén incorporados a un fichero, sea este informatizado o no.

Esto nos permite distinguir este derecho de otros distintos. Por ejemplo, del derecho al honor, del derecho a la privacidad, incluso del derecho a la propia imagen.

Yo a lo mejor podría hacer público, aquí, algún dato de alguna persona. Ese hacer público el dato de una persona, que a lo mejor esa persona misma me ha facilitado no suponía, en principio, violación del derecho a la protección de datos personales. Sería violación de otro derecho, del derecho al honor, a la propia imagen de esa persona.

Si yo no he incorporado ese dato a un fichero automatizado o no, si no ha sido sometido a un tratamiento, repito, el derecho afectado sería un derecho distinto.

Estamos hablando, por tanto, de datos incorporados a ficheros. Datos, y esto es esencial, que son del titular del dato. Y en consecuencia y por definición todos los datos que se incorporan a un fichero son datos ajenos, son datos de terceros, son datos que pertenecen al titular de ese dato personal.

Lo cual explica y da razón de ser a los principios a los que antes me he referido. Muy brevemente: Consentimiento, por supuesto, si estamos tratando datos personales de un tercero es imprescindible que contemos con su consentimiento. En segundo lugar, información, al tratar datos personales de tercero es imprescindible que le informemos que sus datos van a ser sometidos a un tratamiento. Finalidad, evidentemente los datos sólo pueden ser tratados, utilizados para la finalidad para la que fueron recabados y no para otra finalidad. Calidad de los datos, los datos deben ser adecuados, pertinentes, no excesivos, debemos tratar, utilizar, manejar los datos necesarios para el cumplimiento de las finalidades que nos propongamos alcanzar y no más de los necesarios.

Esto nos lleva al principio de proporcionalidad en el manejo de los datos.

Seguridad. Debemos tratar los datos con total y absoluta seguridad, porque, repito, estamos tratando datos de terceros.

Además, es imprescindible que exista una autoridad independiente de control, no sólo porque así se ha considerado oportuno en la Directiva 95 46, no sólo porque así se ha considerado oportuno en las leyes de protección de datos; también la Resolución 45 95 de la Asamblea General de Naciones Unidas del 14 de diciembre de 1990, por la que se establecen las directivas de protección de datos, dispone en su punto ocho que es derecho de cada país designar a la autoridad que vaya a ser responsable de supervisar la observación de los principios de protección de datos. Esta autoridad ofrecerá garantías de imparcialidad, independencia,

frente a las personas o agencias responsables de proteger, procesar y establecer los datos y competencia técnica.

Por tanto, principios esenciales en el derecho fundamental a la protección de datos, que en todo caso deben respetarse, so pena de violentar, como decía antes, el propio derecho.

Este derecho por lo demás está sometido a una serie de tensiones o aparentes tensiones que colocan al mismo en una supuesta encrucijada.

¿A qué me refiero? Se podría decir que el derecho a la protección de datos en estos momentos está sometido a la tensión que deriva de su relación con otros derechos o intereses, con los que en alguna ocasión se ha pretendido o se ha pensado, en mi opinión, erróneamente, que puede haber un conflicto, pero un conflicto desde la incompatibilidad de ambos principios de derechos, cuando eso no es así.

Me refiero a la tensión entre libertad de expresión y protección de datos, tensión entre transparencia y acceso a la información y protección de datos, tensión entre los intereses y evaluaciones del mercado y protección de datos y tensión, por último, entre la lucha contra el terrorismo y garantía de la seguridad pública y protección de datos.

Se ha considerado que la protección de datos es un obstáculo para la seguridad, es un obstáculo para los intereses del mercado, es un obstáculo para la libertad de expresión o para el acceso de información y nada de eso es así.

Es más, en una sociedad democrática, en una sociedad avanzada es imprescindible que la libertad de expresión y la protección de datos vayan de la mano, es imprescindible que el acceso a la información y la protección de datos vayan de la mano, es imprescindible que no se adopte ninguna medida para garantizar la seguridad de los ciudadanos que no tenga en cuenta el respeto a los derechos fundamentales y en particular el respeto a la protección de datos, y es imprescindible que el mercado desarrolle sus actividades y vele por sus intereses con absoluto respeto a la protección de los datos personales.

En dos sentencias del Tribunal de Justicia de las Comunidades Europeas se plantea la atención entre protección de datos y libertad de expresión, protección de datos y acceso a la información.

Me refiero a las sentencias del 20 de mayo de 2003, en el asunto Rundfunk y del 6 de noviembre de 2003, en el asunto Linqdvist. La primera analiza la transparencia y acceso a la información y la relación con la protección de datos; la segunda la libertad de expresión, y en ambos casos, el Tribunal de Justicia de las Comunidades Europeas deja muy claramente sentado que no hay incompatibilidad entre la protección de los datos personales y la libertad de expresión o el acceso a la información; más bien, al contrario, sólo respetando el derecho fundamental de todos a la protección de sus datos personales se conseguirá un marco adecuado de respeto a la libertad de expresión y al derecho de acceso a la información. Un correcto, y añado yo, un correcto desarrollo del mercado y una eficaz lucha contra el terrorismo.

Término lanzando una mirada al futuro, mirada al futuro que debe ser necesariamente optimista.

No podemos dejar de mirar al frente con la esperanza puesta en el uso de las nuevas tecnologías y en la implantación efectiva de la sociedad de la información, superando cualquier brecha digital, pero con respeto absoluto a los derechos fundamentales y entre ellos al derecho a la protección de datos de carácter personal.

El profesor Rodotá, al que cito de nuevo, no hace mucho, el 9 de febrero de este año señalaba que la protección de datos es un elemento fundamental de la sociedad de la igualdad. Es una condición esencial de la sociedad de la participación; es un instrumento necesario para salvaguardar la sociedad de la libertad y un componente imprescindible de la sociedad de

la dignidad, porque esto es esencial. La protección de datos es íntima relación con el respeto a la dignidad de las personas.

Y en este sentido deben ser bienvenidos los procesos regulatorios, deben ser bienvenidos los marcos de referencia normativa, que consigan generar una idea de que, o la idea de que el derecho a la protección a terceros es un derecho fundamental que debe ser respetado, que debe ser regulado y que puede convivir perfectamente con otros intereses, otros derechos, como en particular el derecho al acceso a la información pública, pero teniendo en cuenta que la transparencia administrativa, la administración de cristal no tiene por qué convertir al ciudadano en ciudadano de cristal.

La administración de cristal no tiene por qué convertir al servidor público en servidor público de cristal y, por tanto, tremendamente expuesto a otros riesgos derivados de las sociedades actuales.

Estoy seguro que encuentros como éste servirán para potenciar, para poner en marcha, para continuar con la ilusión y los esfuerzos por conseguir unas sociedades avanzadas y democráticas, en las que el respeto al derecho a la protección de datos, sin perjuicio de otros intereses o valores, sea cada vez más una realidad cotidiana.

Moderador: Fernando Corvera Caraza. Director de disposiciones de *Banca Central* del Banco de México.

Inmediatamente tenemos la ponencia de Joan Crespo Piedra, Director de la Agencia Andorrana de Protección de Datos Personales, es responsable del Departamento de Inspección del Ministerio de Economía del Gobierno de Andorra y es Director de la Agencia Andorrana de Protección de Datos.

Ponente: Joan Crespo Piedra.

El Principado de Andorra es un pequeño Estado independiente, situado en el corazón de los Pirineos, entre dos grandes Estados amigos y hermanos: España y Francia.

Nuestros 468 kilómetros cuadrados dan acogida a una creciente población de 70 mil habitantes con residencia fija y a unos 10 millones de turistas al año.

Tiene una gran industria turística, donde tanto los sectores públicos y privados tienen una gran relevancia.

Nuestro régimen jurídico es una democracia parlamentaria con plena separación de poderes. Nuestra Constitución fue aprobada por referéndum en el año de 1993.

Se puede considerar que la supervivencia del principado se debe al equilibrio jurisdiccional que data de la Edad Media y donde los primeros textos legislativos daban una gran importancia al equilibrio entre los señores feudales, el Obispo Palacio Durgel y el Presidente de la República Francesa, que han garantizado la independencia y la supervivencia de este mismo Estado.

Haciendo mías las palabras que pronunció en su ponencia el señor Fernando Argüello: *vivimos en un mundo en constante evolución, siendo el cambio una constante real e incontrovertible y donde*, añade, *pensar lo impensable es una forma de mover la rueda del aprendizaje*.

En este sentido, el Principado de Andorra ha ido adaptando sus instituciones a la modernidad y a la imparable globalización. Nuestro Estado, que se acaba de integrar a la Red Iberoamericana de Protección de Datos, gracias a la inestimable colaboración recibida de la Agencia España de Protección de Datos.

Teníamos que agradecer este hecho y a los miembros del IFAI la posibilidad de participar en este Encuentro, que seguro aportará nuevas perspectivas, actualizando e intercambiando experiencias, que enriquecerán y ampliarán nuestros conocimientos.

Desde la perspectiva de un pequeño Estado, donde la cultura de protección de datos es de reciente implantación dado que nuestra Ley Calificada de Protección de Datos fue aprobada por el Consejo General, por el Parlamento, en el transcurso del mes de diciembre de 2003 y publicada en el Boletín Oficial del Estado en enero de 2004, teniendo en cuenta que Andorra se sitúa en el contexto europeo, y por tanto, el marco de regulación se sitúa en el ámbito de influencias europeas, dentro del contexto y en el marco de la cultura e influencia de los países vecinos.

Cabe destacar el carácter de autoridad de control independiente de la agencia andorrana, así como hacer un énfasis especial en el hecho que tanto el director como los inspectores están nombrados directamente por el Parlamento andorrano, necesitando para ello una mayoría de tres cuartas partes de los parlamentarios presentes.

Es por ello que la ley andorrana desarrolla los preceptos que vienen redactados en la Constitución a través de sus artículos 14 y 15, a los que he hecho una referencia en la introducción de esta ponencia, y que resumidos recogen el derecho a la intimidad, la privacidad y la inviolabilidad del domicilio, así como a la adaptación de la Ley de Protección de Datos a los preceptos constitucionales, entendiendo el derecho a la protección de datos como lo que es, un derecho fundamental de la persona.

Entre los objetivos que se pretenden, es conseguir una protección adecuada, sin que por ello tenga que ser un costo excesivo para las organizaciones y las administraciones públicas. Y para ello a través de los 44 artículos de la Ley y de las disposiciones Transitorias se garantiza el derecho a la protección de sus datos de los 70 mil habitantes del principado y se regulan asimismo de una forma similar a la que se enlista en los países vecinos y especialmente en el marco de la Directiva 95 46 del Parlamento Europeo.

No obstante la sensibilidad para garantizar este derecho fundamental, se tiene que ir adaptando con la misma rapidez que las nuevas tecnologías. Y es en este ámbito donde los pequeños Estados podemos ir aplicando, más apresuradamente, la legislación a las necesidades y los derechos reales de los ciudadanos, ejerciendo en todas las capas de la sociedad el acceso a la información, el acceso al conocimiento y, sobre todo, a que todos los ciudadanos de todos los niveles sociales conozcan realmente sus derechos, será una de las labores principales a desarrollar y acrecentar.

La agencia andorrana de protección de datos ha iniciado sus actividades en varias direcciones.

La primera, ofreciendo formación a las organizaciones de carácter privado. La segunda, ofreciendo la colaboración necesaria a los ministerios y organizaciones de carácter público, de tal forma que puedan adecuar los ficheros gestionados a una norma de creación aprobada por el organismo competente.

Asimismo, desde la agencia andorrana se están preparando unos seminarios de formación y concientización para que los responsables y los funcionarios de las diferentes áreas adapten adecuadamente sus procedimientos a la legislación de protección de datos.

Paralelamente a estas acciones se van a iniciar unas campañas informativas dirigidas a todos los sectores de la sociedad andorrana, a todos los habitantes del Principado de cualquier nivel cultural, con la finalidad de tejer una telaraña cultural de protección y gestión de los datos de carácter personal, desde la perspectiva inseparable del derecho fundamental a su protección y dentro de la más estricta adecuación y adaptación al margen legal vigente.

Para concluir esta intervención, les agradezco la posibilidad de participar en este Encuentro que aportará grandes y nuevas expectativas a países que, como el nuestro, inician modestamente su andar con el ánimo de que el ciudadano encuentre una respuesta adecuada

en la protección de su intimidad y su privacidad ante las perspectivas que la globalización, las nuevas tecnologías y una necesidad inagotable de expansión de las empresas provoquen alarmas de ataque que pueden ser previstos y anulados desde las agencias estatales de protección de datos independientes.

Desde nuestra perspectiva y teniendo en cuenta nuestra corta experiencia, esperamos ante todo acumular proyectos, asimilar experiencias y en un breve plazo de tiempo aportar a las fuerzas de participación nuestra pequeña experiencia. De manera que el ciudadano consiga realmente el derecho de disposición de sus datos, el derecho de control, el derecho de conocer, el derecho de oponerse y, en definitiva, el derecho de poder ejercer un control real y efectivo de sus datos de carácter personal.

Moderador: Fernando Corvera Caraza. Director de disposiciones de *Banca Central* del Banco de México

Prosiguiendo con las ponencias, tenemos a José Manuel de Frutos, de la Unidad de Protección de Datos, de la Dirección de Justicia, Libertad y Seguridad en la Comisión Europea. Es licenciado en Derecho de la Universidad Complutense de Madrid, tiene diversos estudios complementarios, curso de Derecho Constitucional y Ciencias Políticas de Madrid, curso de Derecho de Empresas en la Escuela de Práctica Jurídica, también de Madrid; en su actividad profesional ha participado en la Comisión Europea; es Administrador Principal en la Unidad de Protección de Datos Personales y ha sido Director del Departamento Internacional de la Asociación Española de Empresa de Seguros. Tiene diversas publicaciones.

Ponente: José Manuel de Frutas.

El señor Piñar ha desarrollado ya de manera bastante brillante lo que es el derecho fundamental a la protección de datos en general.

En el texto que les voy a presentar y que voy a entregar. Este desarrollo histórico figura también en mi ponencia, por lo cual ahora no voy a hablar de ello, voy a entrar directamente en lo que es el marco europeo de la protección de datos, el derecho fundamental de la protección de datos dentro de la normativa europea.

El derecho comunitario en la Unión Europea, en principio, su objetivo fundamental es el conseguir un espacio único en el mercado interior, es el objetivo inicial de los primeros convenios, en el que se trata de garantizar una libre circulación de lo que llamamos los factores fundamentales de capital, trabajo, mercancías y personas.

Dentro de este contexto se generó lo que llamamos el derecho a la libre circulación de los datos personales. Como ha dicho el señor Piñar anteriormente, el objetivo principal era garantizar que el valor económico que tienen los ficheros de datos personales, pudieran ser objeto de libre circulación dentro de ese mercado interior.

Ahora bien, esto no se podía hacer sin que al mismo tiempo se garantizara el derecho a la protección, al derecho fundamental que revisten los datos personales.

Y dentro de esta tensión que existía entre garantizar la protección al derecho fundamental a los datos personales, por un lado, y garantizar el derecho económico a la libre circulación de esos ficheros dentro del mercado interior, es donde surge esta normativa, que es la 95 46, en la que se establece el régimen jurídico que hoy en día impera en la Unión Europea para garantizar el respeto y la protección de los datos personales.

Me gustaría decir dos cosas: Esta primera norma que se ha adoptado en la Unión Europea, en materia a la protección de datos personales, establece una normativa que no cubre todo el ámbito de actuación de la Unión Europea, ni todos los datos personales que pueden tratarse

en la Unión Europea. Esta normativa únicamente se aplica a lo que nosotros llamamos el primer pilar o lo que es lo mismo, a la circulación de datos dentro de la Comunidad Económica Europea, lo que sería el mercado interior.

Existen otros sectores que están excluidos de esta normativa, que son los sectores que llamamos de cooperación policial o judicial penal, que son sectores que se han incorporado posteriormente en el año 93 a la construcción europea, y que no figuran dentro de lo que es el embrión inicial de la construcción europea; como se han incorporado posteriormente, esta parte de la protección de datos queda en principio sometida a normas nacionales en espera de que se adopte una normativa comunitaria que está precisamente en tramitación en estos momentos.

Conviene decir dos cosas, que lo que empezó siendo en las comunidades europeas una normativa que tenía como objeto el garantizar o conciliar la libre circulación de datos personales dentro del mercado interior y garantizar que ello se hiciera de manera adecuada para proteger el derecho para la protección de datos personales, y que era una normativa de carácter más o menos económico, ha trascendido este carácter económico para llegar a ser hoy en día un auténtico fundamental de la persona, reconocido como tal en la Carta de Derechos Fundamentales aprobada en Niza en el año 2000. El derecho a la protección de datos personales es un derecho fundamental a parte entera de la Unión Europea que trasciende lo que es el valor económico a la libre circulación de datos personales.

¿El por qué se da una normativa europea? Ya lo he dicho, es básicamente para garantizar la libre circulación de datos personales. Pero me gustaría hacer referencia al frontispicio de la Directiva 95 46. Los considerando que normalmente, en principio, prefiguran o preceden la parte dispositiva de un acto comunitario, la exposición de motivos, por así decir, se dice de manera muy clara en los considerando números dos y tres, que los sistemas de información, de tratamiento de la información están hechos al servicio del hombre y no al revés, y que lo que se trata de hacer es que estos sistemas de tratamiento de la información tienen que estar establecidos de manera tal que siempre se pueda garantizar la protección del derecho fundamental a la protección de datos personales.

En el considerando número tres se dice que dentro de la Comunidad Europea es preciso garantizar la libre circulación de datos personales, puesto que tienen un valor económico que forman parte de las cuatro libertades fundamentales. Pero que esta libre circulación ha de hacerse en todo momento de acuerdo con el respeto a los derechos fundamentales y al derecho fundamental de la protección de los datos personales.

Y el artículo Uno, de la Directiva 95 46 consagra en letras de molde cuál es el objetivo de esta norma, garantizar y adoptar a la norma una serie de principios que los Estados miembros tienen que incorporar en su derecho nacional para garantizar que la protección de datos personales se lleve a cabo con los principios establecidos en esta Directiva, que adopta los principios comunes para todo lo que son las legislaciones de los Estados miembros.

Y en segundo lugar, una vez que se han adoptado estos principios y que se garantizan que en el derecho nacional se van a respetar, el corolario de este respeto es la posibilidad de que los datos personales contenidos en los ficheros dentro de los Estados miembros puedan circular libremente dentro de la Comunidad, puesto que se va a garantizar que los datos personales están protegidos de manera adecuada en cualquier Estado miembro.

Este es el objetivo de esta normativa y esto es lo que hace que a continuación la Directiva 95 46 que es la norma básica que existe hoy en día en el derecho comunitario, establezca todo un desarrollo normativo que obliga a los Estados miembros a incorporar para garantizar cómo se va a llevar a cabo el tratamiento y el respeto y el

control de los datos personales dentro de los Estados miembros.

De manera esquemática diré que la normativa comunitaria impone dos grandes aspectos, en un primer lugar, lo que prevé es: los datos personales han de ser objeto de una regulación adecuada por parte del responsable de información de tratamiento de los datos, hay una serie de derechos que se garantizan al ciudadano, a la persona interesada y al mismo tiempo se establece un régimen de control y de supervisión.

Régimen de control que supone la asistencia, autoridad de protección de datos independientes y públicas que deben garantizar la supervisión y un régimen de notificación o depósito de los ficheros para que la autoridad de control pueda llevar a cabo lo que es el principio de control de esas bases de datos que existen en los Estados miembros.

Los principios reguladores los ha desarrollado el señor Piñar, suponen que el tratamiento de datos personales, la recogida de datos personales debe hacerse de acuerdo con los principios de licitud del tratamiento, los datos han de ser recogidos para fines precisos, legítimos, explícitos y determinados, deben ser recogidos, bueno, por el principio de proporcionalidad y además, deben ser conservados de manera adecuada y durante el tiempo que sea preciso para la finalidad para la cual fueron recogidos.

Existen normas específicas respecto a la transmisión de datos a terceros responsables y conjuntamente se desarrollan los derechos fundamentales para el ciudadano; para el interesado del derecho a la información saber que sus datos están en principio recogidos en un fichero específico y al mismo tiempo la posibilidad que se otorga al ciudadano para que esos datos que están en un fichero puedan ser rectificados, suprimidos, bloqueados o borrados, según las circunstancias.

Ya he dicho, que en principio la segunda parte de la normativa comunitaria implica que tiene que haber siempre un control de esos datos, control que supone, por un lado, la creación de autoridades independientes y públicas que dispongan de los medios adecuados para llevar a cabo el control de los ficheros que existen en el Estado en el que esas autoridades tienen competencia.

Control que supone la posibilidad de tener poderes para interferir en la acción y poder corregir la actuación que tienen los responsables de los ficheros para corregirlos y hacerlos que se adecuen o respete la normativa vigente en el Estado en cuestión.

Y en tercer lugar, para poder controlar este tipo de datos existe un premecanismo de notificación previo al establecimiento de los ficheros, autoridad de control, para que sea consciente de que existen estos ficheros y pueda llevar a cabo las medidas oportunas del caso de que hubiera quejas o de que ella misma, de oficio, estime necesario poder proceder a una inspección de los ficheros en cuestión.

Me gustaría decir que el principio del derecho comunitario es garantizar un espacio interior en el que los datos pueden circular libremente, la normativa comunitaria contiene también una serie de principios de relaciones de este derecho, de este bloque económico con países terceros y existen una serie de disposiciones muy importantes respecto a la posibilidad de poder transferir datos o no a países terceros.

El principio fundamental es que los datos que se tienen en un fichero en un Estado miembro sólo se pueden proceder o transferir a un país tercero, cuando el país tercero en cuestión, el responsable que recibe esos datos garantiza, mediante su legislación y su sistema jurídico un nivel adecuado de registro de datos personales, semejante o adecuado al que existe en la Comunidad.

Si no fuera así, en principio, esos datos no se pueden transferir a esos países terceros. La Directiva a continuación tiene una serie de normas que permiten que en casos especiales

esos datos se puedan transferir, cuando el interesado así lo consciente, cuando es necesario para ejecutar un contrato en el que el interesado es parte, ese contrato es ejecutado en el extranjero o cuando, en principio, existe una serie de cláusulas contractuales en un contrato establecido entre el responsable del fichero comunitario y el responsable que recibe los datos en el tercer país, en el que se garantiza que el interesado que reside en la Comunidad, por ejemplo, yo, cuando mis datos van a ser transferidos de un fichero comunitario a un fichero en un país tercero.

Esas cosas contractuales que existen en ese contrato, entre los dos responsable que son transmisor y receptor de ficheros, me permiten a mí garantizar que esos datos se me van a respetar y que además podré exigir, en caso de que hubiera una violación o difusión de esos datos a terceras personas, la posibilidad de ejecutar responsabilidades e indemnizaciones por parte de mi tratador de datos en Europa, para garantizar ese respeto de datos personales.

La Comunidad ha llevado a cabo una serie de decisiones de adecuación con determinados países terceros, en el que se ha garantizado o se nos garantiza que determinados países sí garanticen la protección de datos que reciben de ficheros europeos.

Este es el caso, por ejemplo, de Argentina, de Canadá o de la Confederación Helvética.

La Comunidad es una entidad que, en principio, no tiene ningún inconveniente, al contrario, en desarrollar estos acuerdos de adecuación para poder transmitir datos a países terceros y está en principio abierto a que este sistema de adecuación se pueda expandir a otros países terceros.

Por último, quisiera terminar diciendo qué es lo que pasa hoy en día y dónde estamos.

Hoy en día me gustaría decir que estamos, como lo dijo antes el señor Piñar, en una situación de encrucijada, puesto que tras diez años de aplicación práctica de la Directiva en los Estados miembros y de una aplicación que podemos considerar satisfactoria en general, por parte de los Estados miembros, puesto que las legislaciones nacionales funcionan de modo más o menos satisfactorio, nuestra situación actual es de intentar mejorar la aplicación de esas normativas y aplicación por parte de los Estados.

A este respecto estamos cooperando con las autoridades nacionales, para mejorar la aplicación y el cumplimiento de la normativa, por parte de los Estados miembros.

También estamos analizando lo que es el desafío, que supone las nuevas tecnologías, el desarrollo de las nuevas tecnologías y los nuevos mecanismos de tratamiento de la información y cómo ello puede o debe encaminarse dentro del sistema jurídico que ya existe en la Comunidad.

Anteriormente se hablaba de las técnicas AntiSpam, de la vigilancia de técnicas de correos electrónicos, de las identificaciones a distancia por mecanismos informáticos o tecnológicos o de radiofrecuencias.

Son temas que se están analizando, para ver en qué medida hay que llegar a una convergencia que permita garantizar una adecuación o una satisfacción o una acción de la atención que existe entre estos principales informáticos y de tratamiento de información y respeto al derecho fundamental de la protección de datos.

Un tercer aspecto que estamos teniendo hoy en día en la Comunidad Europea es intentar hacer frente al desafío que supone la adopción de normativas específicas, que permitan a los Estados miembros hacer frente a los nuevos retos que suponen la lucha contra el terrorismo, las nuevas formas de criminalidad organizada y cómo los nuevos instrumentos jurídicos o técnicos que se van a dar a las autoridades encargadas de la investigación policial, criminal o judicial penal, pueden o no estar en conciliación con el respeto al derecho fundamental de la protección de datos.

Es una tensión clásica, como dice el señor Piñar, que existe entre estos dos principios: La libertad y seguridad, la seguridad de los ciudadanos frente a la protección de datos personales, la privacidad.

En la Unión Europea no creemos que exista en principio una antinomia, sino que hay que considerar ambos derechos, y prueba de ello son las normas que se están proponiendo recientemente que tratan precisamente de desarrollar un ámbito normativo, en el que se tengan en cuenta estos dos intereses: Protección de los derechos personales, de la protección de datos, por un lado, y normas nuevas que den mayor poder de intervención a las autoridades policiales o judiciales penales para hacer frente a las nuevas formas de criminalidad organizada o de terrorismo.

Y en este aspecto me gustaría citar normas que se están presentando hoy en día, como las que son, por ejemplo, una proposición de directiva que acaba de ser presentada y que está a discusión sobre la retención de datos telefónicos y de correo electrónico por parte de las autoridades, por parte de las empresas encargadas del servicio de telefonía o de correo electrónico para poner a disposición de las autoridades encargadas de la cooperación judicial en el ámbito del terrorismo en el caso de que fuera necesario.

Son normas que están hoy en fase de gestación, en fase de elaboración legislativa y que no sabemos a dónde llegarán.

Moderador: Fernando Corvera Caraza. Director de disposiciones de *Banca Central* del Banco de México

La ponencia estará a cargo de Gerardo Gil Valdivia, Director General de Vinculación Interinstitucional de la Comisión Nacional de los Derechos Humanos; es abogado, tiene estudios de postgrado en Harvard, investigador de tiempo completo en la UNAM; cuenta con diversos libros publicados y tiene actividades docentes en la Máxima Casa de Estudios, el ITAM, Universidad Iberoamericana y la Universidad Panamericana.

Ponente: Gerardo Gil Valdivia.

Quiero agradecer a los organizadores esta oportunidad de participar.

Y tengo dos motivos de especial satisfacción. Inicialmente el poder participar en un encuentro de especialistas, aunque lo que voy a hacer es un planteamiento de carácter general; y suplementario, poder participar en la discusión de este tipo de temas en un momento crucial que vive el país de construcción institucional.

El país ha vivido una serie de transiciones de lo más trascendentales. Unas derivadas de su incorporación en el proceso de globalización. Otras, derivadas de la alternancia política y de la consolidación de su democracia.

En este contexto México tiene un proceso de construcción de instituciones de Estado, de articulación de políticas de Estado que son fundamentales para el futuro desarrollo del país.

La sociedad civil cada vez participa más en este proceso de un proyecto de nación con visión de largo plazo, con visión de un desarrollo sustentable, sostenido, equitativo en el que retomemos la senda del crecimiento económico, en el que logremos este crecimiento económico sostenido con estabilidad, una mayor equidad distributiva en el ingreso, el pleno respeto al medio ambiente con plena vigencia del Estado de derecho y en especial de los derechos humanos.

Y para estos efectos estamos en procesos de discusión, como el de la Reforma del Estado y como el de la articulación de las políticas públicas que nos permitan acceder a la sociedad de la información y del conocimiento, que nos dan plena vigencia en el mundo altamente tecnologizado del siglo XXI.

En este contexto se inscribe, por una parte, la creación y posterior autonomía del Instituto

Federal Electoral que ha sido fundamental para el proceso de alternancia democrática.

La creación hace 15 años de la Comisión Nacional de los Derechos Humanos y su posterior autonomía y consagración como órgano público constitucional de Estado.

La autonomía del Banco de México y, finalmente la creación del Instituto Federal de Acceso a la Información Pública, que es el resultado de dos vertientes de fuerzas. Por una parte, una presión de grupos de la sociedad civil. Cómo olvidar la participación del Grupo Oaxaca en la articulación de esta institución y, por otra parte, en la voluntad política para poder lograr hacer efectivos este tipo de instituciones.

En este contexto quiero inscribir mi participación, simplemente resaltando la importancia que para el desarrollo del país de largo plazo conlleva la articulación de políticas de Estado que estén más allá de las pugnas y de los vaivenes de los actores políticos del momento.

Esta consagración de instituciones hace que este Encuentro sea particularmente importante en el momento de legislar en una materia tan sensible como es ésta, la de los datos personales.

Dicho esto, me limitaría a hacer algunos comentarios sobre el orden jurídico mexicano en cuanto a esta materia. La Constitución Política de los Estados Unidos Mexicanos es omisa en cuanto a la referencia de datos personales, yo me limitaré a referir los artículos Sexto y Séptimo así como los artículos 14 y 16 de la norma suprema.

El artículo Sexto consagra el derecho a la información. El derecho a la información será garantizado por el Estado. Es un artículo que consagra la garantía de que manifiesta, que establece que la manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito o perturbe el orden público y añade el derecho a la información.

El artículo Séptimo de la Constitución también señala que es inviolable la libertad de escribir artículos sobre cualquier materia. Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta que no tiene más límite que el respeto a la vida privada, a la moral y a la paz pública.

Y los artículos 14 y 16 constitucionales, que son piedras angulares del sistema jurídico mexicano, y en particular de la protección de la legalidad y de los derechos individuales, de los derechos fundamentales, que establece que nadie podrá ser privado de la vida, de la libertad o de sus propiedades, posesiones y derechos, sino mediante juicio seguido ante los tribunales previamente establecidos, en los que se cumplan las formalidades esenciales del procedimiento y conforme a las leyes expedidas con anterioridad al hecho, y el artículo 16 constitucional que determina que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente que funde y motive la causa legal del procedimiento.

Por otra parte, el artículo tercero, fracción segunda de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, determina ya el tema de los derechos de los datos personales.

Y los define, como la información concerniente a una persona física identificada o identificable, entre otras, la relativa a su origen étnico o racial, que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales u otras análogas que afecten su intimidad.

La ley considera que los datos personales constituyen información confidencial, y que en consecuencia nunca pueden ser dados a conocer por las autoridades u órganos públicos.

En relación con los datos personales, la ley describe varias obligaciones de los servidores públicos. Este tipo de datos, señala la ley, solamente se podrán solicitar por un funcionario cuando sean estrictamente necesarios para la labor que se desarrolla dice el artículo 20, fracción segunda. Esto significa que ningún funcionario puede requerir de un particular o de otro funcionario datos personales, si no es con base en alguna norma jurídica que lo autorice expresa y claramente.

Pero no basta cualquier regulación normativa para acceder a datos personales, ya que para no ser inconstitucional e ilegal se debe acreditar su razonabilidad y proporcionalidad en razón de su objeto, ya que puede suponer un potencial peligro para un derecho fundamental, como el derecho a la intimidad.

En otras palabras, sólo se podrán pedir datos personales cuando así lo autorice una norma jurídica siempre que sean indispensables para alcanzar un objetivo constitucionalmente legítimo.

Los particulares, cuyos datos personales consten en alguna base de datos en poder de cualquier órgano público, pueden solicitar a la Unidad de Enlace respectiva que se los proporcione.

La ley abunda en la normatividad en relación con los sujetos obligados y con otros aspectos específicos que quizá puedan ser objeto de comentario posterior, y yo me limitaría a señalar que el marco jurídico regula la responsabilidad administrativa de los servidores públicos por el uso indebido de datos personales.

Esta responsabilidad está regulada por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y por la Ley de Responsabilidades Administrativas de los Servidos Públicos.

Otros aspectos que señala el orden normativo que regulan este tema, es la responsabilidad patrimonial del Estado, y que la responsabilidad administrativa de los servidores públicos son independientes de las de orden civil o penal que procedan.

El IFAI tiene entre sus atribuciones establecer los lineamientos y políticas generales para el manejo, mantenimiento, seguridad y protección de los datos personales que estén en posesión de las dependencias y entidades.

Asimismo, quisiera señalar otros aspectos, es particularmente relevante la Ley Federal de Responsabilidad Patrimonial del Estado, debido a la reforma constitucional del artículo 113, en su fracción II, y con motivo de la creación de esta ley es el mismo Estado responsable de indemnizar a los particulares que sufran daños en sus bienes o derechos como consecuencia de la actividad administrativa y regular del Estado, es decir, se genera una responsabilidad objetiva y directa por parte del Estado.

También existen otras normativas aplicables para la protección de esta materia que es el Código Civil Federal, la Ley Federal de Protección al Consumidor, el Código Penal Federal y la legislación financiera.

En cuanto al Código Civil Federal cabe mencionar el daño moral, regulado por el artículo 1916; en cuanto a la Ley Federal de Protección al Consumidor, el artículo 16 señala que los proveedores y empresas que utilicen información sobre consumidores con fines mercadológicos o publicitarios tienen un conjunto de obligaciones en esta materia. En cuanto a la responsabilidad penal de los particulares por el uso indebido de datos personales podemos referir el artículo 350 del Código Penal Federal en cuanto al delito de difamación. Y podemos referir también un capitulo particular de revelación de secretos y acceso ilícito a sistemas y equipos de informática.

Por último, quisiera hacer referencia a la legislación financiera en cuanto a la Ley de Instituciones de Crédito, que regula la confidencialidad de los datos de sus clientes y el secreto financiero, así como la Ley para Regular las Sociedades de Información Crediticia, elemento fundamental para la función normal crediticia de los bancos.

Quisiera simplemente, después de esta visión muy de conjunto y sujetándome al tiempo que se me asignó para esta breve exposición, resaltar la importancia de la consolidación institucional en este proceso de cambio económico y político que vive el país, la importancia de que el IFAI pase a ser un órgano constitucional autónomo del Estado que consolide los esfuerzos que ha venido realizando hasta ahora.

Y la importancia de una regulación adecuada en todo este proceso enmarcado en todo este proyecto de articulación de una visión de largo plazo de nación en el que logremos este desarrollo equitativo, sustentable y sostenido para el país.

Moderador: Fernando Corvera Caraza. Director de disposiciones de *Banca Central* del Banco de México.

A continuación Luis Alberto Domínguez González, que es Consejero del Instituto de Transparencia y Acceso a la Información Pública del Estado de México. Es Catedrático de la Universidad Anáhuac y de la Escuela Libre de Derecho, abogado por la escuela Libre de Derecho y tiene un doctorado en Derecho de la Empresa por la Universidad Complutense de Madrid y la Universidad Anáhuac, en donde se encuentra laborando actualmente una tesis doctoral.

En el ámbito profesional últimamente se desempeñó como Director Ejecutivo del Consejo Nacional de Ciencia y Tecnología, Director Consultivo del Instituto Federal de Acceso a la Información Pública. Ha escrito diversos artículos en materia de derecho a la información, transparencia y acceso a la información pública y protección de datos personales.

Ponente: Luis Alberto Domínguez González.

José Luis Piñar Mañas, Presidente de la Red Iberoamericana, señores comisionados del Instituto Federal de Acceso a la Información Pública, compañeros consejeros del ITAIPEM, miembros de la Red, señoras y señores.

Ciertamente después de todo lo que se ha comentado he de reconocer que me han allanado un tanto cuanto el camino referente a la definición del derecho fundamental de protección de datos personales.

Recapitularé un poco, haré algunas reflexiones y por supuesto emitiré mi punto de vista con respecto a qué es lo que nos falta por hacer en nuestro país.

Ha quedado claro que la protección de los datos personales debe ser considerado un derecho fundamental que ha sido reconocido recientemente, por supuesto que está relacionado con la cuestión de intimidad de privacidad, pero no es lo mismo y debemos de tener mucho cuidado con la distinción, y mucho cuidado porque es así de sencillo: La cuestión del domicilio o la inviolabilidad del domicilio, a la que se refiere nuestra Constitución, propiamente se estaría enmarcando como una de las libertades que tienen las personas y que se constituyen en sí mismas como limitaciones al poder público, para la injerencia precisamente a su ámbito privado. Y eso corresponde a derechos de los denominados de primera generación.

La protección de los datos personales ya se ha enmarcado de facto en derechos de tercera generación. Es decir, ya no es el artículo 16 Constitución, no es el 14, no es el Sexo ni el Séptimo, como ya adecuadamente ha mencionado el ponente que me ha precedido en el uso de la voz. Ese es el punto medular de este asunto.

Entonces resulta preocupante que busquemos una regulación de protección de datos personales basada en estas disposiciones constitucionales, que *per se* tienen una naturaleza de primera generación, cuando ya se ha conformado como una de tercera, en donde ya no es ni intimidad ni privacidad ni propia imagen, sino un derecho fundamental de protección de datos personales, y que está referido a cualquier información relativa a mi persona o a la de ustedes. Efectivamente, está relacionado con las cuestiones de dignidad.

Pero me preocupa este panorama, reitero, que la Constitución Política de los Estados Unidos Mexicanos refleja, sobre todo, si estimamos que este es un tema que ya ha sido analizado y que además, ha evolucionado desde los años ochenta e incluso desde antes.

Ya ha mencionado José Luis Piñar, el Convenio 108; ya también ha mencionado que en Alemania desde el 77 se han hecho cosas al respecto. Incluso en España la Ley Orgánica sobre Protección de Datos de Carácter Personal o LOPD del 92, que fue superada ya por la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal del año de 99.

Y nosotros todavía seguimos esperando a que finalmente logremos una Ley de Protección de Datos Personales.

Me adhiero al comentario de la Comisionada Marván, en cuanto a que podemos celebrar y hacer un reconocimiento al senador Antonio García Torres, por haber puesto este tema en la mesa, creo que es muy importante.

Pero creo que también será importante no solamente la aprobación o la promulgación de una ley de esta naturaleza, sino que incluso yo me atrevería a sugerir reformas de carácter constitucional. Porque, reitero, datos personales no es el 16, no es el 14, no es el Sexto, no es el Séptimo.

Esto implicaría, por supuesto, la regulación y el análisis para efecto de reflejar una garantía individual en la propia Constitución, que nos permita que para que mis datos personales sean protegidos o en caso de que éstos sean violentados, pueda yo acudir a un órgano que no sea un tribunal ordinario. Eso es muy importante.

Y que dentro de la acción de los datos personales no nada más tenga yo la posibilidad, por supuesto, de acceder a ellos, solicitar las correcciones o las supresiones correspondientes, sino que incluso pueda pedir indemnización por daños y perjuicios, en caso de un manejo irresponsable de los mismos.

¿Podemos armonizar el acceso a la información pública con la protección de datos personales? Por supuesto. ¿Podemos armonizar la libertad de comercio con la protección de datos personales? Por supuesto.

No es una cuestión sencilla. Si la cuestión fuera sencilla, no tendría quizá sentido esta reunión.

Lo que sí no tendría sentido, reitero, es limitarnos, al menos en nuestro país, a un análisis en base a textos tradicionales de Derecho Constitucional, que francamente, ante estos derechos de la tercera generación se han visto ya superados.

Ciertamente, ya hay muchos que se han comprometido con este tema y que ya lo están abordando y creo que hay que tomarlo muy en cuenta.

De tal suerte que el estar discutiendo si el nombre, si el domicilio, todos aquellos supuestos que contempla tanto la Ley Federación de Transparencia, como la Ley de Transparencia del Acceso a la Información Pública del Estado de México, son datos personales o no, está de más, está definido en la ley, y habla de otros casos análogos.

Pero, retomando lo que ya se ha venido comentando con anterioridad, es que es mucho más amplio que eso, es cualquier información y es mi derecho el controlar mis propios datos. Es mi derecho.

Y si mis datos ya los he proporcionado, también es mi derecho el que me pregunten si yo quiero que se manejen de cierta forma o no; tengo derecho a que se me pregunte y a que se me informe y a que se me explique qué destino se les va a dar.

Tenemos problemas muy serios, como ya se ha mencionado, con respeto al Centro de Acción y Promoción de la Mujer; tenemos problemas serios en cuanto a la suplantación de personas por contrataciones electrónicas, son suplantaciones virtuales en donde utilizan datos personales para celebrar actos en nombre de otra persona sin su autorización. Esto es muy grave.

Comparto también los conceptos que ha emitido en su momento la Comisión Europea y los tribunales constitucionales, tal como lo comentó el doctor Piñar Mañas, como el derecho a vivir solo. Eso es muy importante.

O como también mencionaba y haciendo especial referencia a los servidores públicos, en mí caso, Gustavo R. Velasco, que finalmente pues existe el derecho a perderse entre las multitudes. Una cosa es la gestión pública y otra cosa es la vida privada y la dignidad de las personas.

Debemos de tener muy en cuenta que el desarrollo de las tecnologías de la información y los conceptos de autodeterminación informativa, libertad de información, libre comercio, los flujos transfronterizos de información son temas que hay que abordar y de manera pronta y seguir reflexionando sobre ellos de manera permanente porque avanzan de una manera abrumadora y podríamos correr el riesgo de vernos superados de nueva cuenta.

Debemos de lograr que se consagre nuestra Carta Magna, este poder de disposición y control de datos frente a terceros, el saber quién los tiene, para qué los tiene y que yo pueda oponerme al uso que se le dé a los mismos.

Por supuesto que esa facultad de controlar y la capacidad para disponer y decidir sobre mis datos personales, reitero, tendrá que ser regulada por una ley; ya hay avances al respecto, que bueno.

Sinceramente yo creo que sino hacemos reformas constitucionales, y reitero también, me aventuro a decirlo y me atrevo a decirlo, esto podría quedar un tanto cuanto incompleto porque es un derecho fundamental que no está como tal regulado en la Constitución Mexicana.

Le daría incluso más fuerza como garantía constitucional, de tal suerte que podamos tener una protección adecuada, nuevamente menciono, sin necesidad de acudir a tribunales ordinarios, sino que tengamos una protección especial sobre la información, por supuesto, cualquiera que ésta sea, sobre mi persona que sea manejada de manera irresponsable o que sea violentada.

No quisiera dejar pasar la oportunidad de agradecer a la Red Iberoamericana de Protección de Datos Personales, a la agencia española, al IFAI la confianza que han depositado en el Instituto Estatal.

Les doy la bienvenida a todos en nombre de mis compañeros del ITAIPEM, hago un reconocimiento a todo el personal del Instituto de Transparencia y Acceso a la Información Pública del Estado de México y, particularmente sí quisiera hacer referencia a la Unidad de Clasificación y Protección de Datos Personales quien desde hace varias semanas ha estado inmerso en la organización de este evento y, bueno, esperamos que sea todo un éxito, así lo creo yo.

Moderador: Fernando Corvera Caraza. Director de disposiciones de *Banca Central* del Banco de México.

La ponencia que nos ocupa está a cargo de Karin Kuhfeldt Salazar, defensora delegada para asuntos constitucionales y legales de la Defensoría del Pueblo-Colombiano. Es abogada graduada de la Universidad de Los Andes, previamente ocupó el puesto de delegada en la Comisión Redactora del Nuevo Sistema Penal y

Directora Nacional de Defensoría Pública; ha sido también profesora de Derecho Constitucional y de Teoría General del Estado en la Universidad de Harvard y dirigió la revista La Defensa de la Defensoría del Pueblo.

Ponente: Karin Kuhfeldt Salazar.

Voy a hacerles un breve recuento de lo que es el panorama del derecho a la protección de datos personales en Colombia.

Lo primero que tenemos que señalar es que no tenemos una ley que siente esas reglas generales de protección del derecho. La Corte Constitucional, por vía de la acción de tutela, que es una acción de protección de los derechos fundamentales, parecida a la solicitud de amparo, es quien ha desarrollado una doctrina sobre lo que puede ser este derecho fundamental.

Sin embargo, para claridad de todos y todas ustedes es importante señalarles que la Corte aún no ha acogido el concepto del derecho fundamental a la protección de datos personales, se refiere al derecho autónomo del *Hábeas data*, como derecho garantía, y se refiere básicamente al derecho a la autodeterminación informática.

El artículo 15 de la Constitución Política establece el derecho de *Hábeas data* en una norma que simultáneamente reconoce el derecho a la intimidad personal y familiar, al buen nombre, a la privacidad de la correspondencia y las comunicaciones en los siguientes términos: Todas las personas tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La Constitución exige que la regulación de los derechos fundamentales se trámite por vía de una ley estatutaria, es una categoría especial reforzada de leyes que exigen una mayoría calificada, un trámite breve en una sola legislatura y, además, una revisión previa por parte de la Corte Constitucional antes de entrar en vigencia.

En el caso del derecho a la protección de datos personales o de *Hábeas data*, como lo ha mencionado la Corte, no hemos logrado en 14 años de la vigencia de la Constitución, y a pesar de la presentación de varias iniciativas legislativas que se apruebe tal norma.

La Defensoría del Pueblo, entidad a la que aquí represento, como órgano constitucional autónomo encargado de la promoción y protección de los derechos fundamentales, ha hecho uso de la iniciativa legislativa que la misma Carta le reconoce, ha presentado ya en tres ocasiones un proyecto de ley sobre la materia, pero seguimos sin tener un texto definitivo.

En este momento cursa en el congreso un proyecto acumulado con el de la Defensoría del Pueblo, y estamos pendientes de ver cuál va a ser el éxito o el fin de esta iniciativa.

Voy entonces a referirme básicamente a lo que ha señalado la Corte Constitucional, que en virtud de la ausencia normativa ha tratado de sentar como unas reglas prefiguradas para poder generar una mínima protección del derecho.

Hay que aclarar que la mayoría de los fallos, más de 130, desde la Constitución del Alto Tribunal, se refieren básicamente a sentencias de tutela, es decir, solamente para casos concretos después de la creación, de la generación del conflicto, y solamente obligan a las partes involucradas en este proceso.

Muy residualmente la Corte se ha pronunciado en sentencias de constitucionalidad, es decir sobre normas, y que tengan carácter, efecto general y que sean de obligatorio cumplimiento para todos los ciudadanos.

En esta medida la protección de los datos personales en Colombia sigue sometida a la libre decisión de intereses económicos y políticos que se mueven alrededor del tratamiento de datos personales.

Como les señalaba, la Corte considera al derecho de *Hábeas data* como un derecho garantía, lo considera un derecho constitucional autónomo, y garantía de otros derechos y libertades fundamentales, en estricto rigor ha señalado que se trata de una garantía a los derechos de autodeterminación informática y de la libertad.

El núcleo esencial de la Hábeas data definido entonces por estos dos derechos se concreta a su vez en la facultad del titular de los datos de autorizar la conservación, uso y circulación de los datos, bajo los parámetros legales que se señalen a tal fin.

Entre los derechos fundamentales protegidos como garantías la Corte ha indicado además de los de intimidad, información, buen nombre, honra y honor, y ha señalado que contribuye a la realización de los valores y principios de la dignidad humana, la libertad y la igualdad.

En consecuencia, y dado su carácter de derecho fundamental su limitación solamente se puede dar por vía de una ley general que señale ese verdadero interés general que responda a los presupuestos establecidos en la Carta de manera que admita una limitación eventual.

En cuanto al concepto, la Corte ha señalado que este derecho otorga al titular la facultad de exigir a las administradoras de datos personales el acceso, la inclusión, la exclusión, la corrección, la adición, la actualización y la certificación de los datos, así como la limitación en las posibilidades de divulgación, de publicación o cesión de los mismos, en armonía con unos principios que forman el proceso de administración de datos personales.

La función de este derecho, ha señalado el Alto Tribunal, es la de equilibrar el poder entre el sujeto concernido por el dato y aquel que tiene la capacidad de recolectarlo, almacenarlo, usarlo y transmitirlo.

Además, la Corte ha dicho que este derecho tiene dos dimensiones distintas y complementarias no solamente las facultades del titular, sino el conjunto de principios que debe guiar todo proceso de acopio, uso y transmisión de datos.

En este sentido, la administración de los datos personales tiene que darse en un contexto claramente delimitado y con sujeción a los principios de libertad, de necesidad, de veracidad, de integridad, de finalidad, utilidad, circulación restringida, incorporación, caducidad e individualidad.

En cuanto al sujeto activo la Corte señala como tal tanto a las personas físicas, como a las personas jurídicas, cuyos datos serán susceptibles de tratamiento automatizado.

La Corte desde un comienzo y en todos los casos ha reiterado que es la persona y no el administrador de las bases de datos el titular y propietario del dato de carácter personal.

El sujeto pasivo será toda aquella persona física o jurídica, pública o privada que utilice sistemas informáticos para la conservación, uso y circulación de datos de carácter personal.

En punto de la conformidad de la administración de bases de datos con estos principios, me gustaría comentarles de una norma que fue declarada inconstitucional, precisamente por violar estos principios de la administración de bases de datos.

En una norma que reformaba el estatuto tributario se planteó la posibilidad, la facultad a la Dirección de Impuestos y Aduanas Nacionales, lo que aquí equivaldría a la Secretaría de Hacienda y Crédito Público tengo entendido, de reportar la información relativa a los deudores morosos a las centrales de riesgo privados.

Es decir, que las centrales de riesgo manejaran la información de quién cumple o no con sus obligaciones tributarias y en qué estado se encuentran.

Con una demanda de la Defensoría del Pueblo a cargo, presentada por la oficina que manejo, la Corte Constitucional declaró inaccesible esta norma, entre varios aspectos señaló que esta disposición vulneraba los principios de finalidad y divulgación restringida del dato, los cuales prohíben esa circulación hacia fines distintos de los que inicialmente fueron los que motivaron la recolección y además permitía la circulación del dato sin la debida autorización del titular.

Finalmente, la Corte también ha señalado que los administradores de bases de datos o de riesgos crediticio y financiero deben informar previamente al titular la incorporación de cualquier información negativa, que le pueda derivar en efectos, limitación de derechos de forma previa a la incorporación de esta información, de tal manera que el titular pueda precaver y evitar daños irreparables que puedan derivarse de la circulación de información errónea.

Quisiera resaltar que si bien la jurisprudencia de la Corte se ha centrado en una gran proporción en los bancos de datos de riesgo financiero y crediticio, ha tocado muchísimos temas relacionados con el manejo de datos por parte de la Administración Pública. Particularmente también se ha referido a las bases de datos que manejan las órdenes de captura o de privación de la libertad.

En el 2003, como ejemplo, se planteó una acción de tutela por parte de un ciudadano a quien le habían librado una orden de detención, que fue posteriormente cancelada, porque había un error en la identidad de esa persona.

Este ciudadano fue objeto de privación de la libertad 20 veces, con base en esta información, simplemente porque la orden de captura nunca fue retirada de las bases de datos, donde según lo había ordenado el mismo juez que lo había liberado.

Y, en este sentido, el ciudadano fue privado de la libertad 20 veces y solamente hasta que llegó a ejercer la acción de tutela, logró que la Corte ordenara retirar su información de la Base de Datos del Departamento Administrativo de Seguridad, DAS.

La defensoría valora inmensamente estos encuentros; estima que la información, los documentos que produce la Red Iberoamericana de Datos, ayuda a muchos países que, como Colombia, en el ámbito Iberoamericano aún requieren la aprobación de una ley con carácter urgente, precisamente para la protección de los derechos de los individuos.

Moderador: Fernando Corvera Caraza. Director de disposiciones de *Banca Central* del Banco de México.

Conforme al programa tendríamos tiempo para responder a un par de preguntas.

Pregunta: De acuerdo con una declaración de la Comunidad Europea, la protección de datos personales es un derecho fundamental y un derecho autónomo.

Respuesta del ponente: Luis Alberto Domínguez González

Yo le suplicaría que me hiciera el favor, porque tengo una duda: ¿Derecho autónomo en qué? ¿Derecho autónomo en cuanto a los derechos humanos?

Aquí, en México, efectivamente, la Constitución Federal no menciona a la protección de datos personales como parte de las garantías individuales.

En el Estado de México nuestra Constitución en el artículo 5, sí establece dentro del derecho a la información la obligación de proteger los datos personales. Ese es el sustento constitucional

local, en cuanto a la protección de datos personales que señala la Ley de Transparencia y Acceso a la Información Pública del Estado de México.

Por eso me entra la duda de: ¿Autónomo en qué? ¿Es fundamental porque está dentro de una Constitución?

Yo creo que aquí, de acuerdo con el orden jerárquico, aceptado generalmente por todos los países, tenemos a la norma fundamental, comúnmente llamada Constitución, que es la que rige y no importa primera, segunda o tercera generación, es la Constitución y sobre esa la tenemos que respetar.

Yo quisiera que me hiciera el favor de aclararme un derecho fundamental autónomo respecto a qué, por favor.

Respuesta del ponente: José Luis Piñar.

Vamos a ver, en efecto, estamos hablando de un derecho fundamental autónomo, utilizando la expresión en el sentido de que no se trataría de un derecho, el de la protección de datos, vinculado al derecho a la intimidad o a la privacidad, sino que logra o coincide, como yo apuntaba, con las reservas que, por supuesto, hay que tener al utilizar esta expresión, emanciparse o diferenciarse mejor del derecho a la privacidad o a la intimidad.

El Tribunal Constitucional español, en esas sentencias que antes comentaba y sobre todo en la Sentencia 292 del año 2000, del 30 de noviembre, lleva a cabo una interpretación, creo que muy interesante acerca de si es posible considerar que el texto constitucional, además de reconocer los derechos fundamentales que expresamente en él están reconocidos, puede además reconocer otros derechos implícitos novedosos, derivados de una nueva interpretación de la Constitución.

En Estados Unidos hace unos años se planteó un gran debate entre Borking y Borck, originalismo *versus* interpretación. Hay que estar excesivamente atado al texto concreto de la Constitución o es posible interpretar la Constitución de acuerdo a las nuevas realidades y a los nuevos derechos que van surgiendo.

Y el Tribunal Constitucional considera que el derecho a la protección de datos, si no estaba expresamente previsto por la Constitución en el año 1978, sí se puede derivar dada la evolución social que se ha producido, sí se puede derivar de la Constitución, entendiendo que del texto constitucional, como indico, pueden también derivar nuevos derechos. Y entre estos nuevos derechos se encontraría el derecho de datos que se diferencia del derecho a la privacidad, a la intimidad.

En los términos que también antes intenté exponer y que se pueden conducir a lo que yo llamaba formulación lacónica del artículo 8 de la Carta Europea de los Derechos Fundamentales, en donde ya no se habla del derecho a la privacidad, no se habla del derecho a la intimidad frente al uso de la informática, sino tan sólo derecho a la protección de datos personales que se traduce en ese poder de disposición sobre nuestros datos, sean éstos referentes a la vida privada o no.

De modo que un dato no privado, un dato no íntimo también estaría integrado dentro de ese poder de disposición que todos los ciudadanos tenemos.

¿Por qué? En definitiva, los datos son nuestros, simplificando al máximo, los datos son nuestros sean éstos o no íntimos y con esos datos, en consecuencia, y perdón por la expresión, podemos hacer lo que queramos y estamos en disposición de que otros los usen o no, siempre evidentemente con límites. Todos los derechos fundamentales tienen límites, evidentemente.

Yo creo que los dos únicos derechos que no admiten límite alguno, son el derecho a la vida y el derecho a la dignidad de las personas. Los demás, todos admiten límite y por supuesto también el derecho a la protección de datos.

Por eso el legislador puede delimitar el contenido del derecho, pero partiendo de la base de que estamos ante un derecho fundamental cuyo núcleo esencial debe ser siempre respetado y esto implica que por ejemplo deba estarse al principio de finalidades o de proporcionalidades cuando se analiza el uso de unos datos o que se deba determinar si realmente, y me remito ahora a las sentencias que antes comentaba del Tribunal de Justicia –Linqdvist & Rundfunk, si realmente es proporcional dar una información o hacer público una información, o si para la finalidad perseguida no era necesario hacer pública una información.

Muy rápidamente, en 30 segundos. La sentencia de Rundfunk, como saben ustedes, se refería por ejemplo a un supuesto planteado ante el caso del control por el Tribunal de Cuentas austriaco, de la gestión de determinadas entidades públicas.

Control que llevaba emparejado el conocimiento, por ejemplo, de las retribuciones de los empleados públicos de numerosas entidades públicas.

Y se planteó la cuestión de si esos datos referidos a la retribución de los empleados públicos, no sólo debían incorporarse al informe del Tribunal de Cuentas, si no que también si debían o no, si podían o no incorporarse al informe público, publicidad total y absoluta, de ese informe del Tribunal de Cuentas.

Y el Tribunal de Justicia dijo que habría que valorar, habría que determinar si la finalidad perseguida, que era la del control de la buena gestión se conseguía sin necesidad de hacer total y absolutamente públicos esos datos, si no que a lo mejor bastaba con que el Tribunal de Cuentas así mismo lo conociese. Y para ello se basa en la existencia de ese derecho a la protección de datos.

Quizá en lugar de autónoma habría que decir diferenciados, quizá autónomo de otros derechos porque es un derecho que se considera nuevo.

Moderador: Fernando Corvera Caraza. Director de disposiciones de *Banca Central* del Banco de México.

¿Si hubiera alguna otra pregunta que deseen formular?

Intervención: Yo soy la titular de la Unidad de Enlace de Productora Nacional de Semillas. Más bien lo que yo quisiera manifestar es una duda, porque si bien es cierto que los datos personales que tiene el organismo, pertenecen, por ejemplo, a sus trabajadores que tiene o que ha tenido, y que solamente la ley nos marca, la Ley de Transparencia que solamente para el uso de los datos personales, el titular de los datos debe dar su autorización o debe de autorizar a otra persona para que los pueda pedir, ¿qué pasa cuando esa persona ya no trabaja en el organismo, pero está buscando trabajo y da un currículum y da referencias, y entonces entra en comunicación con nosotros otra dependencia, otra empresa que le va a dar trabajo, pero pide referencia de él, y nosotros no tenemos la posibilidad de contactar al titular de los datos, y nos encontramos ante una disyuntiva?

Si bien es cierto el titular es el dueño de los datos, ¿qué hacemos, si no damos el acceso a la información, pues a lo mejor no le dan trabajo, porque están pidiendo referencia de él? Y muchas veces las empresas aplican ciertos cuestionarios.

Entonces no sé quién me podría, en un momento dado, decir qué se hace ante esto, de dar o no dar acceso a ciertos datos personales, porque aquí lo que estoy entendiendo es que todos los datos referentes a una persona son datos personales.

Respuesta del ponente: Gerardo Gil Valdivia.

Si entendí bien el planteamiento de la pregunta es: ¿Tenemos el expediente laborar de un ex servidor público, y se están pidiendo referencia de él? ¿O se está pidiendo acceso a su expediente laboral?

Intervención: Son referencias de él y de cierta manera también son datos de su expediente personal, porque, por ejemplo, hay cuestionarios que te aplican, y dicen que si ese trabajador fue sindicalizado o que si ese trabajador sufrió accidentes laborales durante su estancia o bajo qué nivel de tabulador estuvo, cuál fue su último sueldo.

Entonces de alguna manera todos esos datos el propietario es el titular de los datos. Pero te lo piden las empresas porque están pidiendo referencias de esa persona para poderle dar trabajo. Entonces si no se lo das también lo estás privando que le den trabajo.

Pero de cierta manera tú no pues contactar al titular de los datos para preguntarle: oye, autorízame a que yo le diga todos estos datos a esta empresa que me los está pidiendo de ti. Porque se los tuvo que haber dado él, si no la empresa cómo llega a nosotros, y nos pide específicamente datos muy concretos de esa persona.

Respuesta del ponente: Gerardo Gil Valdivia.

Recordemos que hay disposición de la Ley Federal de Transparencia en donde existen ciertas obligaciones que todos aquellos sujetos, valga la redundancia, obligados que tienen que reflejar en página Web. de tal suerte que desde mi perspectiva la cuestión del último salario percibió, la antigüedad del empleado, toda aquella información que tiene que ver con la gestión pública, ojo, haciendo especial referencia a la Ley Federal de Transparencia, como aquella que pudiese establecer desde esta perspectiva la excepción a la protección de los datos, si me permiten la expresión, porque finalmente debemos de entender que es al revés, pero para este caso en particular no habría ningún problema en dar esa información.

Ahora, si tenemos evaluaciones, por ejemplo, si tenemos exámenes sicométricos, si tenemos ese tipo de situaciones y lo que se están pidiendo son documentos, no hay lugar a duda de que eso es un dato personal y no se entrega.

Las tecnologías de la Información y su Impacto en la Privacidad: de las computadoras a las telecomunicaciones

Mesa 2:

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA-México.

El doctor Jesús Rubí Navarrete es abogado. Director del Gabinete del Ministro de Justicia, Director General de Relaciones con las Cortes y el Parlamento Español; Asesor Jurídico del Tribunal de Cuentas; Vocal del Tribunal de Defensa de la Competencia; Subdirector General de Inspección y Adjunto al Director de la Agencia Española de Protección de Datos.

Conferencia Magistral: Jesús Rubí Navarrete.

Me sumarme a las felicitaciones a los organizadores, en particular al IFAI y agradecerles a ustedes su presencia.

En primer lugar querría insistir en una idea que ya se ha manifestado a lo largo de la mañana. Hay que distinguir el derecho a la intimidad y el derecho a la protección de datos personales.

El derecho a la intimidad es el derecho que se refiere a una esfera privada de la persona, mientras que el derecho a la protección de los datos personales en parte presume el tratamiento de la información sobre las personas, hace que esa información no sea secreta, sino todo lo contrario, que sea objeto de un tratamiento, inclusive de un tratamiento masivo, pero exige una conducta activa por parte de los que realizan ese tratamiento y esa conducta activa consiste básicamente en que sea una conducta o un tratamiento con garantías, una conducta garantista.

Esta conducta garantista se traduce en lo que se refiere al objeto de la ponencia. En primer lugar, en el tratamiento de datos automatizados en las computadoras; es el tratamiento de datos que podemos distinguir de otros tratamientos que veremos posteriormente, relacionados con el desarrollo tecnológico.

En este ámbito en que el tratamiento automatizado de los datos personales y el tratamiento en bases de datos, en las computadoras que utilizamos en la perspectiva de la Unión Europea, está sujeto a un sistema de garantías que tiene dos bloques.

Por una parte, los principios de protección de datos, que ya se han comentado, el consentimiento, la información, la calidad, la finalidad, la seguridad o el secreto y una serie de derechos, como son los derechos de acceso, de rectificación, de cancelación y de oposición.

Sin embargo, el desarrollo tecnológico, el desarrollo del sector de las telecomunicaciones y de las nuevas tecnologías ha dado lugar a un hecho nuevo, a que ese sistema de garantías, esos principios que acabo de comentar o esos derechos, necesiten adaptaciones específicas ante nuevos fenómenos tecnológicos.

El desarrollo tecnológico obliga a adaptar los principios de protección de datos, en primer lugar, a la seguridad de la red; obliga a recoger, a considerar qué medidas de seguridad, qué riesgos se producen; cuando se producen esos riesgos la necesidad de informar a los usuarios de que se han producido y también la necesidad de ofrecerles soluciones tecnológicas a un costo razonable, para poder evitarlos.

Los datos de tráfico son aquellos datos que identifican la comunicación que se está realizando y que permite la facturación, es un tratamiento que con las herramientas disponibles Data Warehouse, Data Maning pueden dar lugar a perfiles muy exclusivos en la vida de las personas y necesitan una adaptación de los principios generales de protección de datos a sus peculiaridades.

Y lo mismo sucede con los datos de localización que son los datos que permiten la ubicación física de los equipos terminales y que pueden dar lugar al hecho de que se produzca un seguimiento, un control de itinerancia de los usuarios de esas terminales.

También en el sector de las telecomunicaciones se están desarrollando servicios de valor añadido, desde los más elementales, como puede ser la bienvenida cuando llegamos al aeropuerto de México diciéndonos qué tenemos a nuestra disposición, todo tipo de servicios, información turísticas o simplemente una bienvenida, hasta servicios muy sofisticados que pueden llevar a suponer el tratamiento, por ejemplo, de datos relacionados con un problema cardiaco de una persona y que permita atenderle, inclusive sin que él se esté dando cuenta de que tiene una crisis cardiaca.

Por qué no hablar de las comunicaciones comerciales más solicitadas, el Spam, que constituye uno de los fenómenos más graves en el desarrollo de las telecomunicaciones, como también lo constituyen el desarrollo de programas espías que permiten obtener información de las terminales sin conocimiento de los usuarios o los zombis que permiten inclusive acabar casi suplantando al usuario de un equipo terminal y utilizar su terminal para hacer, por ejemplo, comunicaciones comerciales no solicitadas como si lo hiciera ese usuario que es el titular de al terminal.

Y lo mismo sucede también en servicios avanzados de telefonía, puesto que estos servicios permiten la identificación de la línea desde la que se llama, la identificación de la línea a la que se conecta o permiten el desvió o la retirada del desvío automático de llamadas.

Sucede en esta necesidad de adaptación en los directorios de telecomunicaciones, las guías de telecomunicaciones que es un instrumento que se utiliza con carácter público para el tratamiento de datos personales, o con la facturación desglosada. Por tanto, tenemos una primera necesidad de adaptar esos principios generales vinculados a las propias exigencias de la protección de datos personales, cuando éstos se tratan en el sector de las telecomunicaciones.

Pero además, estas nuevas exigencias vienen derivadas de aspectos que son ajenos o sino ajenos, por lo menos no directamente relacionados con la protección de datos personales, como es el desarrollo de los servicios de la sociedad de la información.

La Cumbre Mundial sobre la Sociedad de la Información que se celebró en Ginebra en el año 2003, marcó una serie de objetivos respecto del desarrollo de la sociedad de la información.

Yo he recogido algunos datos los que me han parecido sintéticamente más importantes en cuanto a la protección de datos personales, como son, que las tecnologías de la información y las comunicaciones, permiten un desarrollo más intenso de la educación, del conocimiento, de la información como todos podemos conocer o también marca un objetivo que es que las tecnologías de la información y del conocimiento, las TIC coadyuvan de una manera muy eficaz al crecimiento económico y en particular inclusive en países en desarrollo, porque permiten alcanzar nuevos niveles de eficiencia y de productividad.

Sin embargo, en esta declaración de Ginebra se hace referencia a que, para que pueda desarrollarse la sociedad a la información existen determinadas necesidades.

Primero. Que haya conectividad, sin acceso a la red no va haber, en ningún caso, desarrollo de la sociedad a la información.

Segundo. Que haya una colaboración, una cooperación entre entidades públicas y privadas y también en el ámbito internacional dirigida a tratar de evitar o de reducir la brecha digital, la de aquellos que pueden acceder a este tipo de servicios y la de aquellos que podrían quedarse al margen de los mismos.

Tercero. Se hace referencia a una necesidad de competencia, de que exista un funcionamiento competitivo de mercado, aunque siempre garantizando obligaciones de servicio universal, porque la competencia puede excluir del acceso a estos servicios a aquellos que vivan en locales o territorios o que tengan niveles de rentas que no permitan su acceso a estos servicios y por tanto los poderes públicos tienen que garantizar o establecer obligaciones de servicio universal que permitan a toda la población el acceso a esos servicios.

Y en particular entre estas necesidades se hace referencia a una que está muy directamente vinculada con la regulación de protección de datos, porque se dice que es imprescindible fomentar la confianza y la seguridad. Sin confianza y seguridad por parte de los usuarios no se desarrollarán adecuadamente los servicios de la sociedad a la información. Y esto implica que haya seguridad en redes, que haya herramientas de autenticación, suficientes, adecuadas, que se garantice la privacidad y que se proteja a los consumidores.

Y hace una referencia específica a la necesidad de abordar estrategias y políticas que permitan por lo menos, sino evitar sí reducir este fenómeno que conocemos como el Spam. En esta declaración de Ginebra se hace referencia a la necesidad de que existe un entorno propicio para el desarrollo de la sociedad de la información, cuyo primer aspecto es que exista un marco jurídico adecuado. Una regulación, en esta materia, que sea transparente, que sea competitiva, que sea tecnológicamente neutral, que sea predecible, y que se adapte, esto es muy importante, a las necesidades nacionales.

Tenemos en este momento dos aspectos o dos puntos de vista que obligan a adaptar los principios de protección de datos a las nuevas exigencias del sector de las telecomunicaciones. Uno es derivado de la propia estructura, del propio sistema de garantías de protección de datos personales.

Segundo, vinculado al desarrollo de los servicios de la sociedad de la información.

Y hay un tercer aspecto, que hace necesario o imprescindible el que exista este tipo de garantías en el desarrollo del sector de las comunicaciones, es el que hace referencia a las necesidades de desarrollo del comercio internacional. Se ha comentado en algunas ponencias que la libre circulación de datos personales es un elemento esencial para el desarrollo del comercio internacional.

Se ha hecho referencia a que en realidad el origen último de la propia directiva 95 46 de la Comunidad Europea, que es una norma vanguardista en lo que se refiere a la protección de datos personales, tuvo ese apoyo en las competencias que el Tratado de la Unión atribuye a la Comisión Europea en materia de mercado único o de mercado interior, el garantizar la libre circulación de datos consideraba y se sigue considerando como imprescindible para que pueda haber un funcionamiento correcto del mercado único, y lo mismo sucede en el ámbito de la Unión Europea, que es una organización regional, y por tanto, esa exigencia responde a las necesidades de integración de esta región o a las de cualquier otra región, podríamos citar el caso americano, el MERCOSUR, por poner un caso, hacen imprescindible que para garantizar la libre circulación de datos exista una regulación que prevea un sistema de garantías, y no sólo en el ámbito de una integración regional, sino también en el comercio que se realiza entre unas y otras regiones, entre todos los países, en definitiva, el tratamiento de datos y la libre circulación de datos personales que se produzca en un mercado globalizado.

Y partiendo de estas necesidades yo querría hacer referencia a abordar los criterios que son necesarios o los criterios que deben dirigir esta regulación en el sector de las telecomunicaciones para poder atender los retos de la protección de datos personales, para poder atender el desarrollo de los servicios de la sociedad de la información, y para poder favorecer el desarrollo del comercio y de la actividad económica a nivel mundial.

El primer aspecto que considero importante o imprescindible que se incorpore en cualquier regulación que aborde esta materia, es que se parta del principio de neutralidad tecnológica. En la experiencia europea hemos tenido un ejemplo claro de los inconvenientes que puede generar el no cumplir con este principio.

La neutralidad tecnológica significa que el sistema de garantías que se establezca sea operativo, cualquiera que fuere la tecnología que se utilice, pueda ser operativo para tecnologías que todavía no han sido desarrolladas.

La primera directiva de protección de datos en la Unión Europea, en el sector específico de las telecomunicaciones del año 97, vinculó el sistema de garantías a determinadas tecnologías, fundamentalmente los servicios telefónicos, y olvidó otros servicios u otras tecnológicas, básicamente el desarrollo de Internet y ha sido necesario modificar esa directiva, derogarla y aprobar una nueva, la Directiva 2002/58-C, para garantizar que este sistema de garantías opera con neutralidad tecnológica.

Y esto es muy importante, porque si no fuera así podríamos encontrarnos con un fenómeno que podríamos denominar de deslocalización tecnológica, si las garantías que existen son distintas para unas tecnologías y para otras, si son más rigurosas en unos casos que en otras, el fenómeno que se puede producir es que se incentiven determinadas tecnologías y se aparquen otras en las que pueda ser más complicado de aplicar este sistema de garantías; por tanto, es un principio fundamental.

En la neutralidad tecnológica el sistema europeo se apoya en un concepto de comunicación electrónica, que es un concepto extraordinariamente amplio, lo tienen ustedes en la Directiva 2002/58-C y que parte de la premisa de que siempre que haya una comunicación electrónica que es simplemente una transmisión de información entre un número finito de personas, cualquiera que sea la red que se utilice, siempre que se produzca ese fenómeno se aplica el sistema de garantías.

El segundo aspecto importante desde el punto de vista de esta regulación o el criterio a incorporar en esta regulación, es que este sistema de garantías tiene que articularse como derecho de los abonados y los usuarios y no como obligaciones de los operadores de telecomunicaciones, ni como obligaciones de los

prestadores de servicios de la sociedad de la información.

Porque si se articula como obligaciones acaban produciéndose déficit y omisiones, por ejemplo, el Spam es algo que realizan terceros que no son prestadores de servicios de la sociedad de la información y que no son operadores de telecomunicaciones, de forma que si establecemos un sistema de garantías basado en un régimen de obligaciones habrá terceros en los que no concurre esas características que hagan Spam y que no estén sujetos a las obligaciones propias de los sistemas de protección de datos o de garantía del tratamiento de datos en el sector de las telecomunicaciones.

Ha habido muchos ejemplos en la legislación española y la nueva Ley General de Telecomunicaciones ha tenido que invertir las cosas, es necesario articular este sistema de garantías como derechos subjetivos de los abonados y de los usuarios oponibles frente a cualquiera, sea operador de telecomunicaciones o no sea operador de telecomunicaciones, sea prestador de un servicio de la sociedad de información o no lo sea.

El tercer aspecto relevante es lo que he querido llamar superación del concepto de dato personal, la normativa de protección de datos personales, como se ha comentado esta mañana, es una normativa sujeta a un aspecto crucial, debe tratarse información de personas físicas identificadas o identificables.

Y esto lleva a un debate permanente de si determinadas informaciones son informaciones sobre personas físicas identificadas o identificables, la dirección IP es un dato de una persona identificada o identificable, un número de un determinado celular es un dato de una persona física identificada o identificable, el propio terminal en el que se pueden instalar virus u otro tipo de programas espías que capten la información supone el tratamiento de información personal identificada o identificable.

En nuestra experiencia tenemos argumentaciones jurídicas que permiten afirmar que la dirección IP, que la dirección de correo electrónico, etc., en determinadas condiciones son un dato personal.

Pero es, en mi opinión, necesario superar este concepto e ir a un sistema de protección que proteja el uso de determinadas herramientas, el uso del teléfono celular, el uso del terminal; porque de esa manera, primero, no va a estar excluido del ámbito de protección nadie cuando se debate si es un dato personal y además, porque se puede incluir dentro del ámbito de protección no sólo a las personas físicas, sino también a las personas jurídicas.

Y la importancia de este aspecto ha sido que el legislador español cuando ha incorporado en nuestro sistema legal la Directiva 2002/58, que es la directiva vigente en la Unión Europea para protección de datos en el sector de las comunicaciones electrónicas o de las telecomunicaciones, ha desvinculado este sistema de garantías del concepto de dato personal y lo ha incorporado en dos regulaciones distintas, una parte en la Ley General de Telecomunicaciones y otra parte en la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico.

Y ha atribuido, eso sí, nuevas competencias a la Agencia Española de Protección de Datos de forma que ahora no sólo aplica lo previsto en la Ley de Protección de Datos, sino también, este régimen de garantías predicable inclusive de personas jurídicas o morales que está en la Ley General de Telecomunicaciones y en la Ley de Servicios de la Sociedad de la Información.

Otro aspecto muy importante a considerar para un enfoque o una regulación en el ámbito del sector de las telecomunicaciones es el dotarse o el prevenir herramientas que puedan ser útiles para combatir este fenómeno auténticamente inquietante, que son las comunicaciones masivas o comunicaciones comerciales o no comerciales, los correos electrónicos no solicitados, el Spam.

Ese punto es un problema particularmente amplio en la medida en que vivimos en un mundo globalizado, pero yo sí querría destacar tres aspectos en los que hemos estado trabajando.

En primer lugar el de conseguir una adecuada colaboración entre las autoridades de control, los prestadores y los usuarios.

Frente al Spam no basta con que exista un régimen sancionador, porque puede no ser aplicable, porque el Spam está en un lugar al que no se puede aplicar extraterritorialmente una norma. Por tanto, no basta con una regulación. Es necesario, pero no es suficiente.

En segundo lugar, es necesario contar con los prestadores de servicios de la sociedad de la información, a través de los cuales está circulando este tipo de comunicación y además, es necesario contar con la concienciación y una actitud proactiva por parte de los propios usuarios, tienen que ser conscientes de la importancia de este fenómeno, de los riesgos que corren y como decía, desarrollar una conducta activa de autoprotección.

Y, demás, de esta manera, mediante esta interrelación, se pueden resolver problemas jurídicos importantes. Por ejemplo, si los prestadores de servicios de la sociedad de la información autónomamente establecen sistemas de filtrado de los correos electrónicos, va a suceder inapelablemente que habrá falsos positivos y falsos negativos; habrá correos electrónicos lícitos, que son retenidos y que llegan a sus destinatarios y seguirá habiendo correos electrónicos ilícitos, que sí llegarán a sus destinatarios.

Y eso puede dar lugar, inclusive, a responsabilidades contractuales, a responsabilidades por daños, a sanciones administrativas por interpretación de las telecomunicaciones, en la medida en que sea una decisión autónoma de los prestadores de esos servicios.

Por eso es imprescindible que los prestadores de estos servicios y las autoridades competentes tengan una relación muy fluida con los propios usuarios, les informen de cuáles son los instrumentos de filtrado que los prestadores de servicio puedan aplicar; en la aplicación de esos servicios de filtrado tengan la confianza de que jurídicamente están actuando de una manera lícita, para lo cual, es imprescindible la intervención de las autoridades administrativas competentes y además haya respuesta por parte de los usuarios, para que ellos digan y decidan si quieren o no el filtrado, conforme a qué criterios o conforme a qué no criterios o si quieren utilizar herramientas alternativas, por ejemplo, disponer de dos direcciones distintas de correo electrónico, para tratar de evitar este fenómeno.

Es necesario, por tanto, esta colaboración, y esto nos lleva a que es necesario también una concientización de los usuarios, que van a tener que adoptar medidas propias de adquisición y de búsqueda de programas actualizados, de firewall, de programas que eviten el contagio por virus y que el propio usuario va tener esta disposición proactiva, para autoprotegerse.

Y en tercer lugar es imprescindible un aspecto básico, que es la cooperación internacional. Sin cooperación internacional es imposible perseguir el Spam.

Yo he puesto algunas referencias, algunas iniciativas que hemos tenido. Un memorándum de colaboración entre la Agencia Española de Protección de Datos y la Federal Trade Commission de los Estados Unidos de Norteamérica o también el London Action Plan, que es un plan de acción en el que están participando autoridades competentes de protección de datos, de defensa de los consumidores muy variadas, empresas privadas, etc., para que tratar de combatir este fenómeno.

Y un último aspecto importante a considerar, en cuanto a estos criterios, de un nuevo enfoque en el sector de las telecomunicaciones es el relacionado con el gobierno electrónico.

La tecnología, el gobierno electrónico, el E-government o la administración electrónica va permitir un acceso más sencillo a los ciudadanos, va permitir mayor transparencia, va permitir también una mayor eficacia, una mayor eficiencia en la actuación de las administraciones públicas. Pero estos programas de E-government tienen que estar, en todo caso, sujetos a garantías específicas.

Y estas garantías específicas, yo querría hacer referencia a alguna de ellas, a la vista de lo que ha sido nuestra experiencia práctica.

En primer lugar, que haya sistemas de identificación unívoca razonables de los usuarios a distancia de este tipo de servicios, porque sino, pueden acabar produciéndose suplantaciones en el acceso a información administrativa por parte de terceros, que no son los usuarios autorizados.

En segundo lugar, que el tratamiento de la información dentro de las administraciones públicas tienen que responder al principio de finalidad. Y en el ámbito de la administración pública el principio de finalidad se concreta en que los datos que pueden recabarse y que pueden tratarse tienen que estar vinculados al ejercicio de competencias, de atribuciones específicas que se hayan reconocido a ese órgano, a esa parte de la administración pública. No toda la administración pública, por muy pública que sea y porque toda en general responda a razones de interés publico, tiene porqué tener acceso a toda la información disponible. Es imprescindible que se cumpla el principio de finalidad, que se vincule al ejercicio de sus competencias. Y esto es particularmente importante cuando el desarrollo de estos sistemas llega a un nivel de interoperabilidad.

En tercer lugar, es imprescindible que se introduzcan medidas de seguridad que impidan o que mantengan íntegra la información y que impidan accesos no autorizados o si éstos se producen que permitan su detección.

En cuarto lugar, hay que evitar, con estas medidas de seguridad, que con el cúmulo de información administrativa y la utilización de nuevas tecnologías, sea la propia administración pública la que se dedique a realizar perfiles de la conducta de los ciudadanos en sus relaciones con la administración.

Estos son, a mi juicio, los aspectos básicos de un nuevo enfoque en protección de datos en el sector de las telecomunicaciones. El próximo paso, ¿cuál es? La Red Iberoamericana.

En la Red Iberoamericana, precisamente en este IV Encuentro hemos elaborado un documento de trabajo sobre gobierno electrónico y telecomunicaciones. En ese documento de trabajo se detallan para cada uno de estos aspectos que les he ido comentando, el Spam, los servicios avanzados de telefonía, los datos de tráfico, los datos de localización, los directorios y el gobierno electrónico, etcétera, soluciones y propuestas concretas que entendemos que pueden permitir alcanzar un nivel de garantía adecuado.

Es un documento que vamos a discutir a lo largo de estos días y respecto del que tendremos que llegar a conclusiones cuando acabe este encuentro. Espero que hagamos un debate fructífero que puedan tenerlo pronto a su disposición.

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA-México.

Vinculado con el tema que se señaló de varias de las razones por las cuales urge una regulación en lo relativo a las bases de datos personales, vino a mi mente otra temática y otro esfuerzo internacional que ahorita está preocupando a la comunidad internacional, que es precisamente la cuestión del crimen internacional organizado.

La Convención de Naciones Unidas, relativa precisamente al crimen internacional, contempla la temática de las bases de datos y

en concreto y vinculado con toda la temática del lavado de dinero y el narcotráfico, está la cuestión de la cooperación judicial o la cooperación entre los Estados.

No se podrá cumplir con ninguna de las metas o de los objetivos u obligaciones de los propios Estados de no darse una normatividad precisamente que sea acorde a las necesidades que por un lado tienen, en el lado de la balanza, lo que es el derecho a la privacidad y los derechos humanos de la persona, y por el otro lado la tecnología que a muchos ha sobrepasado en varios Estados, lo que es la propia legislación interna y el esfuerzo de la comunidad internacional por controlar y regular debidamente y que se realicen en el campo de lo lícito y no de lo ilícito varias actividades y comportamientos que desgraciadamente no se han sujetado a control.

Quiero presentar al siguiente ponente, el doctor Fernando Argüello Téllez, especialista en normativa regulatoria y asuntos de competencia; doctorado en Derecho Patrimonial por la Universidad Pompaifraba de Barcelona, España. Miembro de la Red Iberoamericana de Protección de Datos, especialista en protección de datos personales en diversos cursos y seminarios; obtuvo el premio de periodismo en 2003 sobre la protección de datos personales, convocado por la Agencia Española de Protección de Datos, ponente de la XXVII Conferencia Internacional de Privacidad y Protección de Datos realizado Suiza, en el mes de septiembre de 2005.

Ponente: Fernando Argüello Téllez. Superintendencia General de Electricidad y Telecomunicaciones del SIGET de El Salvador.

Quisiera agradecer a los organizadores la capacidad de convocatoria que se ha tenido para un tema que es tan novedoso y tan relevante en lo que es el desarrollo de la democracia de todos los países.

Quiero empezar contándoles lo que me pasó por la mañana. Me encuentro con que el vecino de al lado a la habitación del hotel, tenía puesta la tarjetita que siempre ponen en la puerta de: "Por favor no molestar" o "Haga la habitación". Me llamó la atención ya que en este caso, dice: "Privacy please", en vez de "Not disturb".

Y creo que sería interesantísimo que tuviéramos una tarjetita así como en *Monopolio* o *Gran Banco*, para poderle sacar a los encargados y responsables de los tratamientos una tarjetita para decir: por favor respete mi información personal.

Vamos a empezar con la ponencia, con lo básico, que es Warren and Brandeis, ya el Director de la agencia se refirió a él. Esto lo llevo a colación en lo que respecta a lo que son los inicios de las tecnologías en la comunicación, se empiezan a desarrollar la fotografía, los periódicos, pues resulta que ya ahí en 1890 ya surgen determinados problemas con lo que es la privacidad de las personas.

Al parecer la esposa del señor Brandeis había tenido una fiesta social muy bonita, en los medios salió publicada, y resultó que los comentarios que se hicieron no les agradaron. Tenemos una magnifica ponencia en el Harvard Review mostrando lo que es el derecho a la privacidad y que ahora es esencial citarlo prácticamente en todas las ponencia de datos que puede haber.

También estamos hablando de 1972, algunos hechos relevantes. RL Polk & Co., una compañía norteamericana en Detroit, poseía datos personales de alrededor de 130 millones de personas, pudiendo tras un adecuado tratamiento informativo establecer complejos perfiles individuales. Ahí estamos hablando del inicio de la computación; ya podía haber algún tipo de tratamiento de información, pero todavía no habíamos llegado a ese enlace entre lo que eran las telecomunicaciones con las computadoras y la capacidad que tienen éstas de tratar información al respecto.

Más adelante, a finales de los años 80, principios de los 90 empieza en sí lo que sería la

convergencia informática y las telecomunicaciones.

Las tecnologías de la información, como son la utilización de las computadoras para almacenar, procesar datos; tecnologías de telecomunicaciones, como son los teléfonos, transmisión de señales de radio, de televisión, tecnologías de redes de Internet, con su forma más conocida, tecnologías móviles, voz sobre IP (VOIP). Entonces surge la convergencia entre el Internet y estas tecnologías, y se constituye como un medio de comunicación eficiente y de muy bajo costo, que va a facilitar la interrelación entre ellas. Se logra una integración entre lo que es datos, vídeo, tráfico de voz, etcétera.

Una de las nuevas tecnologías que han surgido a través de todos estos avances es el GPS, un sistema global de navegación por satélite, que nos permite determinar en todo el mundo la posición de una persona, un vehículo, una nave, con un error de alrededor de cuatro metros. Las aplicaciones que hoy puede tener son múltiples: navegación terrestre, marítima, aérea, para labores de rescate y salvamento, ubicación de enfermos discapacitados, para rastreo y ubicación de vehículos robados, entre otros.

Otra de las formas de utilizar esta tecnología es para el rastreo de los empleados, para ver las rutas de los transportistas y se utiliza un sistema GPS para poder determinar su posición, se utiliza para evitar robos, para evitar que se salgan de su ruta, etc., pero también pueden ser tecnologías que irrumpan o invadan la privacidad.

Un caso interesante que hay en Internet. William Bradley Jackson fue sospechoso de haber matado a su hija y enterrado su cadáver, las autoridades andaban tras su pista desde hacía mucho tiempo, al enterarse de que las autoridades ya andaban muy cerca de lograr determinar dónde se encontraba el cadáver decidió cambiarlo de ubicación, lo que desconocía es que las autoridades habían instalado un chip de rastreo en su vehículo. Pasaron 10 días, durante ese tiempo llegó Bradley sacó el cadáver de la hija y lo fue a enterrar a otro lugar.

Al cabo de varios días retiraron las autoridades el chip y a través de la información que leyeron pudieron detectar el lugar exacto donde había sido enterrada, por supuesto lo apresaron y a final de cuentas quedó condenado.

Lo que se vio es la disyuntiva entre la necesidad y cómo tendrían que haber actuado las autoridades; se necesitaría haber requerido de orden judicial para hacer este tipo de acción o bastaría con una mera sospecha para poder poner un chip o cualquier forma de rastreo. Para este tipo de casos podrían ser muy útiles, me parece, y nadie podría negarlo, pero también podría ser utilizado en otro tipo de usos.

Otro de los ejemplos es el implante de chips, esto lo están ocupando en algunos países para evitar robos, secuestros, se instalan los chips para estar totalmente ubicados en cualquier lugar del mundo; hubo en Inglaterra un caso bastante siniestro que se pensó en la instalación de chips a los hijos menores para evitar que fueran objeto de cualquier tipo de secuestro.

La voz "sonoripés" es un ejemplo interesante de lo que son estas nuevas tecnologías; como ya les comentaba, es un abaratamiento de lo que son los precios de las llamadas telefónicas, nuevamente interesantes, se está viendo con mucho interés los diversos reguladores de telecomunicaciones, sin embargo, como tecnología relacionada con Internet tiene sus problema de privacidad y seguridad. Al igual que un correo electrónico puede ser rastreado en Internet igualmente la voz puede ser rastreada en Internet.

El FCC, Federal Communications Commission, está tratando de ampliar el campo de una ley la cual permitía el poder acceder a las telecomunicaciones vía teléfono normal, ahora lo quiere instaurar a lo que es voz sobre IP, esto está sobre cargando, en alguna medida, a los proveedores de servicio de Internet, está utilizando el ancho de banda y causando algunos tipos de perjuicios.

Y nuevamente volvemos a lo mismo, me parece muy bien que traten de evitar cualquier tipo de terrorismo internacional, delitos y demás, pero hasta qué punto llegamos.

Debemos preguntarnos cómo identificar y regular la delicada línea que puede separar un uso adecuado de las nuevas tecnologías de la información y las comunicaciones de lo que sería un uso arbitrario en el ámbito de la privacidad y la protección de datos.

Sobre eso podríamos pensar en empoderar al titular de la información personal, a través de la educación, hacer del conocimiento de que son sumamente necesarias, que existan normas claras, un asentimiento informado que es esencial, porque muchas veces los usuarios firmamos cualquier cosa o donde dice autorizamos ceder los datos a equis y ye persona, sin embargo, desconocemos para qué van a ser cedidos.

También hay que fomentar las tecnologías garantistas de la privacidad que se están desarrollando y van en muy buen camino, que también son un elemento bastante atractivo.

Les quiero pasar un video, creo que refleja lo que es el problema que se podría dar en un uso inadecuado de las comunicaciones. Se llama Spears and Pizza y es hecho por el America Cibers Liberty Marius de los Estados Unidos.

(Proyección de video en inglés)

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA-México.

Corresponde ahora al doctor Sergio Antonio Toro. Es Director Ejecutivo de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia, su país natal. Ingeniero en Electrónica por la UNAM, Universidad Nacional Autónoma de México; Maestría en Ciencias de Computación de la Fundación Arturo Rosemblueth. Ocupó cargos en diferentes instituciones bolivianas, destacándose el Ministerio de Hacienda, la Dirección General de Impuestos Internos, el Gobierno Municipal del Alto y Ministerio de Desarrollo Municipal. Ha sido consultor internacional en varios países de Centroamérica, Sudamérica y África.

Sus inicios profesionales se refieren al Distrito Federal, México, donde trabajó por más de seis años en el Instituto Nacional de Cardiología, Dr. Ignacio Chávez y en el Hospital Metropolitano de la Ciudad de México.

Ponente: Sergio Antonio Toro.

Quiero agradecer a los presidentes, al IFAI, y a México donde me he formado, también quiero agradecer al doctor Piñar Mañas por la inclusión dentro de la Red Iberoamericana de Protección de Datos.

Voy a empezar mi presentación haciendo una reseña de qué es lo que se está haciendo en mi país, qué es lo que se está haciendo en Bolivia.

Voy a decir qué es la ADSIB, suena como remedio, pero no es un remedio, son palabras un poquito difíciles, es la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.

La Agencia Boliviana para el Desarrollo de la Sociedad de la Información en Bolivia nace en el año 2002, en el marco de un decreto supremo, no nace como una necesidad o como un tema de que la voluntad política del momento esté de acuerdo con ella, si no más bien como un tema, yo lo calificó como una especie de esnobismo. Todo alrededor, todos los países circunvecinos empiezan a desarrollarse en lo que se llama la sociedad de la información, en tratar de proteger sus datos, en ver la importancia que en el mundo tiene las telecomunicaciones y las TICS y, bueno, hay una declaración que ha sido mencionada hoy, la declaración de Santa Cruz de la Sierra donde varios presidentes, en mi país, firman el convenio para iniciar todas estas labores de proteger los datos personales.

En ese sentido nace una agencia, pero nace una agencia un poco sui géneris porque nace sin presupuesto.

Debido a la situación política que vive el país, el 21 de septiembre del 2004 la presidencia del Congreso Nacional asume tuición de la Agencia para el Desarrollo de la Sociedad de la Información, esto nos hace una entidad sui géneris, una entidad que nos hace transversales a los dos poderes: Ejecutivo y Legislativo, y ahí es cuando empiezo a tener el cabello cano porque tengo de jefes o personas que se creían mis jefes, a todos los diputados y senadores de mi país. Entonces, casi pido la habilitación de un nuevo asiento dentro de mi Parlamento, porque yo me la vivía dando informes que trabajando en mi oficina.

Realmente se me criticó o se criticaba en temas de tecnología de información y comunicación de por qué se utilizaba el gov con ve chica, como government, en lugar de gobierno con be grande como lo tienen en México, por ejemplo. A ese nivel de ridiculez he tenido que responder informes del Parlamento.

La ADSIB no nace sin un presupuesto, cosa curiosa y para suplantar y para vivir de un presupuesto nos hacen el ISP oficial del Estado boliviano y somos los encargados de sistematizar la información, generar políticas estándares del desarrollo de la sociedad de la información en el país, es por eso que estamos aquí presentes.

Nace a partir de dos instancias que existían en el Gobierno boliviano, una de ellas es la UFI (Unidad de Fortalecimiento Informático), que es una unidad que queda del Y2-K. Y otra unidad que es el BolNet, era el que tenía los servicios de Internet en Bolivia, tiene el monopolio del registro de dominios en Bolivia, tiene la administración de los números IP para el acceso a Internet y tenemos los temas de proyecto de conectividad al interior del Estado boliviano.

En ese sentido ADSIB y BolNet son las dos entidades que dan sostén técnico y financiero y que se pueda trabajar fundamentalmente en el tema de la "ticks".

Trabajamos difundiendo las "ticks", haciendo políticas, haciendo la coordinación en el área "tick", tenemos bastante trabajo, y nos nombran operadores oficiales de la estrategia boliviana de reducción de la pobreza dentro de Bolivia en el uso de las "ticks".

Trabajos básicamente, los ingenieros nos gusta hablar en difícil igual que los abogados, en la parte de la derecha, significa que trabajamos en el Setuse o sea, ciudadano a ciudadano, en el gobierno a negocios, en el gobierno a gobierno y en el gobierno a ciudadano, tratando de trabajar en esos campos fundamentales, limitamos nuestra acción. –Se refiere a la presentación que realiza en PowerPoint–

La finalidad de la ADSIB. Somos la encargada de promover políticas, todo lo bonito que puede decir un decreto de creación. Tenemos una misión, que es una misión bastante difícil en un país tan conflictivo como Bolivia. Favorecer las relaciones del gobierno con la sociedad boliviana mediante el uso de tecnologías adecuadas, realmente una misión bastante difícil la que nos ponen, con un país, donde voy a demostrar a continuación tiene muchas gradientes diferenciales.

En la ADSIB nos toca, y le pongo la palabra de ingeniería política, porque Álvaro Díaz de la CEPAL, en su informe a la CEPAL, dice que en la ADSIB se ha hecho una ingeniería política, donde jugamos con los dos poderes. Donde básicamente a mí me toca jugar con los dos poderes.

Yo califico ese jugo como hijo de padres separados, hoy tal cual un adolescente malcriado que cuando me convenía iba con el Ministro de la Presidencia y cuando me convenía me iba con el Presidente del Congreso Nacional para conseguir voluntad política.

Dentro de esa voluntad política hemos conseguido entregar resultados a corto plazo, a mediano y a largo plazo. Uno de los resultados de los cuales me siento más orgullo es que hemos hecho la estrategia boliviana de tecnologías de información y comunicación para el desarrollo.

Hemos participado, hemos elaborado el anteproyecto de ley de comunicación electrónica de datos, firmas digitales y comercio electrónico, se llamaba en un principio, en la versión 63 y ha perdido las firma digitales en el camino, ya se llama comunicación electrónica de datos y comercio electrónico. Participamos en la Red Clara, participamos en Telecentro y otros proyectos más.

En la dificultad vemos la oportunidad de trabajar. Tratamos de aprovechar la coyuntura política para aprovecharnos de eso justamente, de lo que es la voluntad política. Participamos internacionalmente en la Red Geal, en la Red Clara, en la Red Infolac, en la Cumbre Mundial de la Información, y nuestra participación reciente es dentro de la Red de Protección de Datos.

La realidad boliviana no muestra que pertenecemos a un país multiétnico, pluricultural, con más de 50 etnias agrupadas en tres regiones claramente definidas, que se han autodefinido así, poca participación ciudadana en los circuitos económicos del país, especialmente de pueblos originarios, lo que ha marcado la exclusión social, no somos problemáticos, porque sí queremos ser problemáticos.

Tenemos un alto grado de necesidades básicas insatisfechas en el país. Tenemos un país con altos índices de pobreza y marginalidad.

Tenemos la inexistencia de un marco jurídico para el desarrollo de alternativas tecnológicas que ayuden a cerrar la brecha digital. Mucha inversión y apoyo, muchos quisieran tener la inversión que tiene Bolivia, pero cuando está mal orientada y mal organizada se convierte en un fenómeno que yo lo califico "Túpac Amaru"; como Túpac Amaru tuvo una muerte por cuatro bestias, una amarrada a cada uno de los brazos que jaló para un lado distinto. Un poco eso es lo que nos está pasando en este momento con Bolivia, porque tenemos la cooperación jalándonos en distintas direcciones y no nos está permitiendo avanzar como país.

Entonces que ordenar esa cooperación internacional. Somos un país geográficamente muy disperso. Tenemos un millón de kilómetros cuadrados, tenemos 328 municipios, 29 mil localidades pobladas, donde 43 por ciento de éstas no tienen servicio de electricidad.

Y aquí es un dato que habiendo tenido mi formación en un país como México, un país tan democrático como México es un tema que realmente me desgarra y me muestra el país distinto que tenemos, el país con los gradientes que mencionaba que tenemos.

Ahí hay una fotografía en la cual dos autoridades originarias del altiplano y uniformados tras la firma del Programa de Igualdad de Oportunidad, fue el 20 de abril del 2005, este año, primera vez después de casi 200 años de vida republicana que un indígena puede acceder a entrar a un colegio militar, los indígenas no tenían derecho a ingresar ni a universidades, ni al colegio militar, este año se da la igualdad para que los pueblos originarios y los campesinos puedan tener educación militar.

Entonces, ese es el país discriminador del cual les estoy hablando y el país discriminador que presenta niveles de conflicto.

Simplemente llamo a la reflexión que la brecha digital entre los países es de 390 a 1 entre los países desarrollados y los países en desarrollo y esta brecha está aumentando.

El PIB de los cinco países de la CAN, los cinco países de la CAN juntos producen un tercio de lo factura Microsoft, quiere decir que la información sí había sido un buen negocio.

El bienestar dentro de una economía global está basado en el conocimiento de individuos solos, ojalá sea ese individuo que está encargado en la espalda de su madre el individuo que pueda alcanzar un mayor desarrollo dentro de la sociedad futura.

Los reportes de telecomunicaciones muestran indicadores muy buenos, vemos una creciente

desde 1997, muy racional, evidentemente se han instalado teléfonos y se han instalado puntas de conectividad en el país, pero de qué me sirve un teléfono tarjetero en medio de un camino, donde no hay ni las tarjetas, donde no hay posibilidades de desarrollo para la región circunvecina.

La participación de los municipios en Bolivia es de apenas un 51 por ciento del país por departamentos que tienen acceso a Internet.

Bolivia en el área urbana o en el eje central, como llamamos, tiene un índice de 0.48, más o menos equivalente al índice de brecha digital que se tiene entre Chile y España, no estamos mal en las ciudades del eje. Sin embargo, si vemos el porcentual en el área rural vemos que estamos con un 0.96, una diferencia catastrófica entre lo que es ciudad y lo que es campo.

La diferencia al interior. La brecha digital al interior de lo que está sucediendo en Bolivia es más dramática que la brecha digital de Bolivia versus los otros países, tenemos dos países, me permito calificar un país del siglo XXI y tenemos un país que está tratando de entrar al siglo XVII, si es que así se puede calificar.

Pese a eso tenemos la inclusión del Hábeas data que, bueno, la primera Constitución de Bolivia es de 1826, ahora en el marco de los conflictos que se están sucediendo en mi país se habla de una asamblea constituyente donde se va a hacer una reforma total, esperemos que para bien.

Se tienen 17 intentos de reformas, se tiene una Ley de Necesidad de Reformas del año 2002, se tiene una inclusión en el 2004 dentro de la Constitución Política del Estado y se tiene una organización del texto, un texto ordenado en el 2004 también.

El Hábeas data dentro de la Constitución Política del Estado de Bolivia está incluida en un solo artículo, en el artículo 23, y tiene en el párrafo uno, tiene las características y derechos, en los párrafos dos, tres y cinco, tiene los procedimientos para el recurso de Hábeas data y en el párrafo cuatro tiene la incompatibilidad para levantar el secreto en materia de prensa.

Los derechos y deberes fundamentales pese a la inclusión del Hábeas data en el artículo 23, no aparece como un derecho fundamental a la intimidad personal y familiar de las personas, entonces ahí ya estamos vislumbrando un posible problema de nuestra inclusión del Hábeas data dentro de nuestra Constitución.

Las características del Hábeas data. La más importante posiblemente es que está, me parece que surge un poco forzada; es que está redactada en términos negativos, es de carácter procesal para la petición de datos personales, etc.

El acceso de datos a la persona, ratificación, corrección, información obtenida o almacenada, eliminación o exclusión, son básicamente los derechos que tiene cada persona.

Las omisiones que tiene. Es un tema que causa preocupación fundamentalmente, no son subsanadas en la Constitución Política del Estado: la confidencialidad de datos personales y la actualización de datos personales, no son incluidas.

El procedimiento, y aquí hay otro problema dentro de nuestro Hábeas data es que toma a la Corte Superior de Distrito o Juez en Partido, esto es a la necesidad del recurrente. No hay una entidad destinada a hacer la protección de datos, sino son las instancias existentes ya en el país.

Esa es la primera sentencia constitucional, un poquito de la historia, donde el Hábeas data lo contraponen con la Ley de Imprenta y la Ley de Prensa, donde el fallo aprueba la resolución de improcedencia, al corresponder la aplicación de la Ley de Imprenta.

Hay una especie de desconocimiento o una especie de mala aplicación de la Hábeas data o una mala interpretación por parte tanto de los demandantes, como por parte de las entidades que estarían encargadas de la protección de datos.

En cuanto a la legislación relacionada, existe la Ley de Telecomunicaciones, existe el Código Penal, existe el Código Civil, el Decreto Supremo de Acceso a la Información Pública, que menciona el Hábeas data como tal y el Anteproyecto de Ley de Comunicación Electrónica de Datos, que también ya menciona la protección de datos y menciona la Hábeas data.

Las conclusiones que podemos decir en cuanto a nuestra Hábeas data, se precisa una Ley Orgánica para el desarrollo de la misma.

Nosotros queremos aprovechar la coyuntura del Anteproyecto de Comunicación Electrónica de Datos, para hacer el Reglamento específico de la protección de datos personales. Esa es la conclusión principal a la cual puedo llegar y este es el trabajo en el cual estamos abocados en este momento.

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA-México.

Presento al doctor Fernando Martínez Coss, licenciado en Economía por la Universidad Autónoma Metropolitana. Ingresó al sector público en 1983 y desde 1986 se encuentra en la Secretaría de Hacienda y Crédito Público, en donde ha colaborado en el desarrollo de herramientas de apoyo para el cumplimiento de obligaciones fiscales, como Declara-SAT, utilizando para el cumplimiento la presentación de la Declaración Anual de las Personas Físicas, así como la instrumentación de mejoras en servicio de atención a contribuyentes, como los módulos de atención integral a los mismos, esquema de pagos electrónicos de impuestos, sistema integral de comprobantes fiscales, así como la instrumentación de la Guía para Trámites Fiscales y es actualmente responsable del proyecto de la Firma Electrónica Avanzada y Factura Electrónica.

Ponente: Fernando Martínez Coss.

El tema que les voy a compartir esta tarde básicamente versa sobre la firma electrónica avanzada y cómo el Servicio de Administración Tributaria, al cual pertenezco, ha visualizado la forma en la que en la interacción con los contribuyentes podamos tener una relación segura que sea sencilla y, sobre todo, que lleve a una forma de interacción que permita ampliar la cobertura de servicios que tiene el Servicio de Administración Tributaria.

En ese sentido el SAT ¿qué es lo que ha hecho y en qué ha basado su desarrollo? Básicamente ha basado su desarrollo actual desde el año pasado y hasta la fecha, en un esquema que se ha denominado de firma electrónica avanzada.

El primer entendimiento que quisiera que tuviéramos es, ¿qué es una firma electrónica avanzada? Es un conjunto de datos, en este evento estamos hablando de datos, pero sobre todo lo que hemos buscado nosotros como autoridad fiscal es que haya alguien atrás de los datos, que haya una identidad, que haya una persona que de forma segura nos permita tener una relación con el contribuyente. Esto es lo que hemos hecho.

Y la firma electrónica avanzada nos lo ha permitido, de hecho es algo que dentro del marco jurídico que nosotros tenemos ya se encuentra reconocido, es decir, ya tenemos reconocido dentro del Código Fiscal de la Federación los certificados de firma electrónica avanzada.

Con esto abrimos un campo muy interesante a efecto de tener esta relación segura que les comentaba. En este sentido no podría yo estar hablando de un certificado y menos de impuestos si no estuviéramos frente a una obligación.

En nuestro país existe desde el año pasado, el año pasado de manera opcional, la obligación para las personas físicas y las personas morales de contar con un certificado de firma electrónica avanzada.

Este certificado tiene, básicamente, dos segmentos de contribuyentes obligados que es personas físicas con actividad empresarial, con ingresos superiores a un millón 750 mil pesos.

Y el segundo. De personas físicas con actividad no empresarial, entiéndase los arrendadores, los sujetos de honorarios con ingresos superiores anuales a 300 mil pesos y, nuestra legislación, el Código Fiscal consagra un segmento, el cual por su capacidad administrativa no tendrían esta obligación; esto no quiere decir que no pueda optar por ella, en este caso básicamente referido a los contribuyentes del sector agropecuario.

Es decir, tenemos una legislación que nos habilita la posibilidad de tener transacciones seguras, con entes identificados, y me falto un tercero que son las personas morales, que son sujetos ya obligados de presentar, de contar primero con un certificado de firma y de llevar a cabo transacciones electrónicas.

En este sentido tenemos un mecanismo que tecnológicamente nos habilita. Tenemos un marco jurídico que lo define y nos define a los sujetos, pero aquí lo importante es un entendimiento claro. Cuando estamos frente a un certificado de firma electrónica de qué estamos hablando, qué quiere decir esto.

Les quisiera decir que es el equivalente a lo que hoy por hoy tenemos como nuestra firma autógrafa, pero en el mundo de las transacciones electrónicas o en el mundo del Internet.

En mi firma autógrafa yo solo la puedo hacer; sin embargo en la firma electrónica yo solo la sé. Hay una característica fundamental en los certificados que es que en su creación deben de hacerse en absoluto secreto, nadie lo debe de conocer.

Mi firma autógrafa en el mundo del papel es el equivalente a mi certificado de firma electrónica en el mundo del Internet y especialmente en el ámbito de lo fiscal. Es decir, todo lo que tenga que ver con obligaciones fiscales o el mundo de lo tributario tiene un equivalente que se llama certificado de firma electrónica y que tiene básicamente tres características, que es: voy a tener un certificado, voy a tener una llave privada, un mecanismo de acceso seguro y voy a tener una clave de seguridad.

Es decir, en el mundo del papel utilizo lo que ustedes tienen, su pluma y papel y en el mundo electrónico voy a tener estas características que son un archivito punto *cer*, un punto *key* y una llave de seguridad. Esas son las analogías que quisiera que tuvieran.

Ahora bien, ¿cómo le vamos a hacer? ¿Cómo le va a hacer el Servicio de Administración Tributaria para lograr dotar a los contribuyentes de todo esto? Tenemos un mecanismo que es presencial, en donde básicamente lo que buscamos es garantizar la identidad del contribuyente que va a estar atrás de un certificado.

Para este fin lo que le pedimos al contribuyente es que acuda con nosotros previamente validando datos, validando datos de identidad del contribuyente. En los datos de identidad el Servicio de Administración Tributaria tiene la reserva legal de no entregarlos ni revelarlos, esto lo consagra el artículo 69 del Código Fiscal de la Federación, en donde se guarda absoluta reserva de los datos proporcionados por los contribuyentes.

Nosotros no podemos revelar absolutamente ningún dato. Sin embargo, sí nos garantiza que tengamos del otro lado de la computadora a una gente que conocemos, que sabemos quién es y a la cual le podemos proveer un servicio o simplificar que es nuestro objetivo todo esto.

¿Cuál es el ciclo de generación? El ciclo de generación es el contribuyente nos agenda una cita, ahí iniciamos a verificar los datos de identidad del contribuyente.

Segundo, nos llena un requerimiento del lado fiscal suena fuerte, pero finalmente es llenar algunos datos de la identidad del contribuyente, esto lo hace en absoluto secreto. El SAT no conoce las características de esa llave privada que genera el contribuyente. Nosotros no tenemos control de esto. Actualmente tenemos cerca de 370 mil certificados ya generados hacia los contribuyentes, esto nos habla de un número ya importante.

Tengo el dato de la Agencia Tributaria española, que me hablaba el año pasado de cerca de 300 mil certificados generados. En el ámbito de nuestro país estamos ya rebasando ya los 370 mil certificados.

Nos habla de un proceso de cambio paulatino, un proceso de cambio que no hemos hecho, como lo viene previsto en la disposición porque generaría, creemos nosotros, un cambio cultural muy fuerte.

Lo hemos hecho paulatinamente, de forma tal que un aspecto fundamental en estas tecnologías sea la asimilación del cambio tecnológico de forma pausada.

Esto creemos que lo hemos venido logrando con este tipo de cuestiones. El contribuyente, me regreso al ámbito del que estoy platicando, genera su requerimiento, acude con nosotros, vemos que efectivamente se trate de quien es, que es quien dice ser.

Esto lo aseguramos con nuestra información, la cual contamos con el contribuyente, y finalmente, jurídicamente lo que hacemos es cerramos el ciclo.

Es decir, tenemos ya una persona física o moral plenamente identificada y con esto le entregamos un certificado de firma, con el cual podamos llevar a cabo transacciones electrónicas.

Aquí hay una característica fundamental en lo que el SAT ha hecho. Esto, nosotros como autoridad fiscal lo pudimos haber hecho de manera autónoma, sin embargo, el legislador el año pasado previó a un tercero, que en este tipo de fórmulas se le reconoce como confiable, a efecto de garantizar la transparencia de todo esto. En este caso es el Banco de México, en el caso de nuestro país, nosotros, como autoridad fiscal, estamos proponiéndole a Banco de México, cuáles van a ser nuestras prácticas de certificación de identidad.

Es decir, no actuamos de manera autónoma. Eso nos da la absoluta transparencia. Aún siendo autoridad, nosotros, en este caso nuestro país, los legisladores, previeron la posibilidad de que aún siendo autoridad fiscal hubiera un tercero confiable. En este caso fue el Banco de México, a quien le estamos dando estos certificados.

¿Y con esto a qué estamos llegando? Esto habilita desde el mundo de lo tributario a una serie de servicios. Es decir, si en el mundo del papel lo que hacemos nosotros con nuestra firma autógrafa es suscribir o aceptar obligaciones o ejercer derechos, en el mundo de lo fiscal tenemos este escenario, que ahorita es el que vamos caminando.

Es decir, los contribuyentes ya pueden optar por un comprobante fiscal digital, ahí ya estamos teniendo un cambio, un comprobante fiscal digital que en el mundo del comercio electrónico viene a minimizar todas las operaciones.

Con este medio seguro la administración tributaria le permite el acceso al contribuyente a sus datos, es decir, los contribuyentes en nuestro país ya tienen acceso a la información que en materia fiscal el SAT tiene, esto que si lo hubiésemos pensado de manera presencial resultaría algo complejo, hoy por hoy ya es una realidad el que el contribuyente de manera electrónica y remota pueda accesar a sus propios datos.

Adicionalmente, ya lo comentábamos, está la presentación de la declaración anual, los agentes aduanales en operaciones de comercio exterior ya utilizan este tipo de mecanismos.

Y para el año que entra ya tendremos que utilizar este mecanismo de certificado de firma electrónica en los pagos provisionales, es decir, el cumplimiento de obligaciones periódicas que venimos haciendo ya tendrá que ser a través de este mecanismo.

Y bien, si estamos hablando de un encuentro de datos, pues, finalmente yo quisiera cerrar mi

charla con el acceso que pueden tener los contribuyentes mediante este certificado a sus datos, creo que es algo que es muy valioso, sobre todo para los contribuyentes el saber, digo, si hay alguien que conoce de los contribuyentes o de los ciudadanos en este país creemos que es la autoridad fiscal.

Nosotros aglutinamos una gran cantidad de datos que están reservados, sin embargo, lo que ofrecemos ahora es la posibilidad de que sea el contribuyente quien los conozca, que sepa qué es lo que nosotros tenemos, en este caso es la aplicación que hoy por hoy existe en la página del Servicio de Administración Tributaria, en donde a través de estos tres datos: Registro Federal de Contribuyentes, lo que es la contraseña, lo que es su certificado y lo que es su punto *key* la llave privada, puede tener acceso a todos los datos que el SAT tiene de los contribuyentes.

Esto creemos que es una oportunidad muy valiosa que no lo permite y no lo habilita la tecnología, pero sobre todo, que nos garantiza que del otro lado de la computadora hay alguien que es conocido, que nos garantiza la absoluta integridad y que no tenemos la posibilidad de que haya la corrupción de estos datos o que haya el jaqueo de estos datos, son transacciones cien por ciento seguras.

Tecnológicamente, como dato para que ustedes lo tengan, este tipo de llaves son de mil 24 bits, cosa que nos da la amplia seguridad de que difícilmente se podrían jaquear y que nos dan la tranquilidad de quien accede a estos datos es quien debe ser.

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA–México.
Continuamos con la presentación de Alfredo Reyes Krafft, doctor en Derecho por la Universidad Panamericana, Director Jurídico de E-Bussines en BBVA-Bancomer, Presidente de la Asociación Mexicana también de Internet.

Ponente: Alfredo Reyes Krafft.

Yo quisiera retomar un poquito el tema de la mesa y en particular bordar un poquito sobre la misma, estamos hablando de las tecnologías de la información y su impacto en la privacidad, el tema es de las computadoras a las telecomunicaciones.

Yo ahora quiero de alguna manera comentar que estoy representando a la industria de Internet en particular en México y en ese sentido yo quisiera aclarar una cuestión, la tecnología o las tecnologías de la información y comunicaciones, Internet, es un medio, no es un fin en sí mismo; es decir, no podemos hablar de ética de Internet, sino tenemos que hablar de ética de las personas que utilizan este medio que se llama Internet o tecnologías de la información, como quieran llamarle.

Y en ese orden de ideas tendríamos que distinguir entre el uso de la información, el bien informático como un concepto jurídico o técnico y también el bien informático o la informática como instrumento para realizar un determinado acto o un determinado acto jurídico.

En ese contexto y sobre ese punto de referencia no debemos dejar de considerar que Internet es un medio, no es un fin en sí mismo, estamos hablando de las personas.

Ahora, también debemos considerar el tema de privacidad. Nos queda muy claro que la privacidad y el derecho a la protección de los datos es un derecho fundamental, es un derecho fundamental de las personas.

Y en este sentido, este derecho fundamental debe también estar en equilibrio con otros temas también importantes, como serían los intereses de mercado, la libertad de expresión, el libre flujo de información, así como cuestiones relativas al lavado de dinero y lucha contra el terrorismo.

Considerado entonces así y tomando en consideración también el tema que y Fernando,

hace un minuto, había comentado en relación a la delicada línea. Es decir, él hacía referencia a algunas mejores prácticas y a los efectos secundarios que estas mejores prácticas pudieran llegar a tener.

Y tomando en consideración el tema y platicando en particular del tema del Spam, yo creo que también debemos de tomar el punto de referencia.

Por un lado, dentro de Spam se está exigiendo que los proveedores de servicios de Internet cuenten con mejores prácticas de protección y de prevención ante ese problema grave: Filtros anti-Spam, detección y registro de entidades riesgosas, conformación de grupos especializados para su combate, distribución de herramientas, campañas de concientización, atención muy pronta ante reportes.

Pero los efectos secundarios que podemos encontrar ante una situación como ésta, sería el tema a que ya hizo referencia también el expositor anterior de falsos positivos; el tema relativo, por ejemplo, a la diferencia entre Spam y mercadotecnia directa; que los filtros pudieran, en un momento dado, atrapar mensajes que pudieren ser válidos o también el hecho de que la propia auditoría, respecto de los mensajes que yo estoy realizando en los buzones de mis clientes, pudiera considerarse una violación a la privacidad de cada uno de los usuarios.

A final de cuentas no es culpable el proveedor de servicios de Internet respecto de este esquema. A final de cuentas el Spam le genera un problema muy grave al proveedor de servicios de Internet; ocupa ancho de banda del proveedor, el volumen de almacenamiento en cuanto a niveles de almacenamiento es a costa del propio proveedor y no lo puede incidir en el costo por el servicio que está prestando.

Independientemente de eso el ISP no debe dejar de garantizar al usuario una eficaz entrega de mensajes, confidencialidad y respeto y respuesta ante reporte de abusos.

¿A final de cuentas a qué queremos llegar con esto?

Nos queda muy claro que debemos de cuidar este derecho fundamental de privacidad y respeto a la privacidad de las personas. Nos queda muy claro también que en México contamos con legislación, si bien dispersa en algunas entidades o en algunos esquemas, contamos con legislación sobre la materia.

Es muy importante y no es por querer evitar un esquema legislativo, sino por el contrario, es muy importante propugnar por una legislación congruente sobre la materia.

¿Y a qué me refiero con congruente?

Voy a poner tres ejemplos que se han suscitado, a raíz de una Iniciativa de Ley Federal de Protección de Datos Personales, que fue presentada por un senador en México, Antonio García Torres, en febrero del 2001 y fue aprobada por el Senado de la República.

Vamos a poner un ejemplo típico. Un esquema de *opt-in* el requerimiento de un consentimiento previo y expreso de la persona, a la cual se van a tratar estos datos.

Por otro lado, también y dentro del contexto legislativo y como una política de carácter presidencial, tenemos la promoción de la inversión de pequeñas y medianas empresas en ese contexto.

¿Qué es lo que queremos hacer?

Estamos obligando a las empresas a utilizar medios de promoción para las mismas, que puedan generarle un mayor costo, porque requerirá un consentimiento previo y expreso de cada una de las personas, a las cuales les enviarán la información, publicidad o esquema comercial. Y, por otro lado, procuramos incentivar la inversión de estas empresas generándoles un costo.

Otro esquema. El esquema de la prohibición al flujo transfronterizo de datos personales. Se establece en la normativa que queda prohibido el flujo transfronterizo de datos a entidades o países que no cuenten con un nivel de protección, cuando menos equivalente al que se está planteando en ese contexto.

¿Cuál es el problema que tenemos? Contamos con un Tratado de Libre Comercio con América del Norte, con Estados Unidos y con Canadá en donde se establece que no se va a limitar este flujo transfronterizo de datos personales.

No estamos en contra de la legislación. No estamos en contra del respeto a este derecho fundamental de protección de datos personales, lo que buscamos es hacerlo congruente con nuestro esquema jurídico.

Moderadora: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA–México.

Para terminar la doctora Katitza Rodríguez Pereda, Directora del Computer Professionals Social Responsibility –CPSR– de Perú. Su trabajo consiste en analizar disposiciones sobre derechos de autor en el entorno digital, incorporados en el Tratado del Libre Comercio entre Estados Unidos y los países andinos, las propuestas presentadas por los Estados relativos a los derechos de autor en las negociaciones sostenidas en el seno de la Organización Mundial de Propiedad Intelectual y las directrices sobre la privacidad elaboradas en el subgrupo de privacidad del Grupo de Comercio Electrónico, del Foro de Cooperación Económica Asia-Pacífico; también es responsable de coordinar los reportes de privacidad en España y Latinoamérica y de mantener comunicación con autoridades en protección de datos, funcionarios públicos y organizaciones de la sociedad civil en Iberoamérica.

El tema de su presentación es la protección de datos personales y las medidas de protección tecnológicas, piratería de obras contra piratería de datos personales.

Ponente: Katitza Rodríguez Pereda.

Antes de pasar a mi exposición, quisiera hacer dos precisiones; decir que como consumidores debemos exigir que las empresas antes de tratar nuestros datos deban exigirnos el consentimiento previo, informado de que efectivamente deseamos que traten nuestros datos.

Segundo. Si hay países como los europeos que los Estados se preocupan por proteger los datos personales de sus ciudadanos, es justo que si ellos quieren hacer negocios con otros países, el mismo nivel de protección se les den a esos países.

En este panel sobre tecnologías de la información y su impacto en la privacidad voy a tratar un tema importante pero poco conocido, salvo entre aquellos que siguen o han seguido de manera más o menos constante este tipo de casos.

Se trata de la recolección y tratamiento de datos personales que se efectúa a través de las medidas de protección tecnológica o medidas de autotutela incorporadas a las obras protegidas por los derechos de autor.

Antes de que irrumpiera en la vida diaria las tecnologías de la información y que se difundiera el fenómeno de la digitalización, no existía relación directa entre protección de datos personales y derechos de autor.

Una adquiría un libro o disco, lo leía, releía, lo hojeaba, escuchaba la música una y otra vez, todo ello en forma anónima. Hace 20 años no existía cruce de caminos y menos colisión entre protección de datos y derechos de autor.

Actualmente con el desarrollo de las tecnologías de la información y en particular de las medidas de protección tecnológicas el vínculo entre ambos derechos personalísimos se entrecruza cada vez más.

¿Qué sucedió en el entretanto? La digitalización de las obras protegidas por derecho de autor, el abaratamiento de los medios de reproducción y la Internet han facilitado enormemente la publicación, copia, distribución y comunicación al público no autorizada de obras protegidas por el derecho de autor, lo que ha originado que el índice de infracciones a estos derechos sea elevado, y que exista perjuicio económico para los autores y productores.

Lo que se ha traducido, a su vez, en un incremento sostenido y real de los niveles de protección legal de los actuales modelos de negocio en este campo, llegándose al extremo de utilizar el derecho penal, las más graves de las disciplinas jurídicas para reprimir conductas que discutiblemente son consideradas ilícitas.

Como los intentos por disminuir o detener la copia no autorizadas de obras mediante los cauces legales han sido fallidos, ello dio pie a que los titulares de derechos de autor optaran por implementar las denominadas medidas de protección tecnológica, orientada a auto tutelar sus derechos.

En términos sencillos las medidas de protección tecnológica son una suerte de candados virtuales que permiten restringir o controlar el acceso y/o uso de las obras protegidas por el derecho de autor. Estas medidas tecnológicas pueden estar en el sistema operativo, en el software aplicativo, en el hardware o en una combinación de ellos.

Generalmente cumple las siguientes funciones: controlan el acceso a la obra, impiden las copias no autorizadas de las mismas, e inclusive la copia privada, que es un derecho del consumidor.

Autentica la obra con el titular de derechos de autor, e impide que la obra sea alterada, modificada, transformada.

Lamentablemente estas medidas de protección tecnológicas también suelen ser utilizadas por los productores fonográficos y de audiovisuales para controlar los usos que los consumidores hacen, por ejemplo, de los discos, películas y libros digitales.

Pueden registrar el número de veces que se ve una película, escuche un disco o lee un libro digital. Permite verificar si éstos son alterados, copiados, impresos, guardados y permiten restringir, no, perdón, ellos dicen administrar el acceso de una obra.

En síntesis, para los titulares de derecho de autor la respuesta a los desafíos presentados por la tecnología sólo puede estar en la propia tecnología. Sin embargo, las medidas tecnológicas suelen operar violentando nuestra privacía e irrespetando el tratamiento de datos personales.

¿Qué ha pasado con el uso de algunas medidas de protección tecnológica? Pérdida del anonimato. Asistimos al desarrollo de una era en la que progresivamente disminuye el anonimato, no por buenas razones o porque nos hayamos convertido en famosos, sino porque nos está siendo arrebatado por una cultura en la que nos solicitan que nos identifiquemos para todo, en particular para usar los bienes digitales.

Una vez que el anonimato se pierde, los titulares de derecho de autor argumentan que tienen derecho a explotar dichos datos, por tanto es necesario reafirmar la necesidad de permitir transacciones anónimas o con seudónimos en Internet. Esto ha sido establecido por el grupo de trabajo del artículo 29 desde su recomendación sobre el anonimato en Internet, aprobado el 3 de diciembre de 1997, en el que se concluye que el almacenamiento de datos personales en la Internet tiene que respetar los principios de protección de datos personales, al igual que en el mundo “Of line”.

Otro tema. El Código de Identificación Único. Existen medidas de protección tecnológicas que asignan un código de identificación único al contenido o al reproductor de contenidos, y que adjuntan información personal de los usuarios para la identificación y otros fines desconocidos.

Por ejemplo, el Media Player de Microsoft tiene embebido un identificador único global, que permite rastrear a los usuarios. Similar al iBook Reader, también de Microsoft, pide al usuario activar el software y vincularlo a una cuenta de password.

Luego Microsoft captura una identificación de hardware único de la computadora de los usuarios.

El código de identificación único puede almacenar los datos en un fichero, interconectar información personal de diversa índole y vincularla, por ejemplo, como información financiera, obtenida al momento de pagar con tarjeta de crédito o personal, dirección de la oficina, casa, teléfono y mail.

Tercer punto. Recolección innecesaria, información personal, gustos y preferencias de consumo.

Algunos candados tecnológicos van más allá recopilando información personal sobre los hábitos y preferencias de consumo y no sólo saben quién es usted o quién puede ser usted, sino cuantas veces repite la misma escena de una película, qué partes de la película, información que almacena nadie sabe por cuánto tiempo.

Windows Media Player, crea un fichero log, registro, del contenido de las visitas de un usuario IP a un servidor central para obtener títulos de contenidos.

Según el Electronic Privacy Information Center el vincular la información personal identificable con el contenido puede traer como consecuencia una discriminación en el precio, ésta es la venta de un bien digital a precios diferentes a consumidores diferentes.

En el caso, por ejemplo, de Napster To Go, el usuario realiza un pago mensual que le otorga acceso ilimitado a una biblioteca de archivos musicales al que puede bajar y transferir música a otro equipo.

iTunes de Apple, vende *track* individuales de música y los archiva en un álbum, música que sólo puede ser tocada en un equipo específico.

En ambos casos las medidas de protección tecnológicas permiten llevar un control de las actividades del consumidor, frecuencia, orden del uso de las canciones, entre otros, información que nada tiene que ver con el fin primario de proteger los derechos de autor, sino que son recogidas para fines comerciales de *marketing* directo o cualquier otro interés que pueda tener la industria.

En suma, el uso de medidas de protección tecnológica que no respeta los principios básicos de privacidad configuran una situación, por un lado, de ejercicio abusivo del legítimo derecho que tienen los titulares del derecho de autor a proteger su obra, pero que además es trasgresor de los principios de protección de datos personales.

En otro contexto muchas de estas medidas de protección tecnológica serían consideradas spyware.

En conclusión, para suprimir la piratería de obras protegidas por el derecho de autor no debe apelarse a la piratería de datos personales.

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA–México.

Si la mesa me lo permite podríamos dejar unos 10 minutos para responder preguntas.

Pregunta: Mi nombre es Tlacaí Jiménez, soy el titular de la Unidad de Transparencia e Información del Instituto Electoral del Estado de Jalisco.

Mi pregunta es para los señores José Rubí Navarrete y Alfredo Reyes Krafft, si pudieran darme su opinión y versa respecto de algo que en lo personal me pasó hace unos días; como funcionario público lógicamente tengo una dirección de correo electrónico, pero desde hace

varios años vengo manejando una cuenta personal en Yahoo, esta compañía tiene, los que somos usuarios de ella, convenios con Northon para antivirus y un filtro anti Spam.

Hace unos días revisando mi correo veo un título que dice invitación a foro o invitación a congreso, no recuerdo ya bien las palabras, me llamó mucho la atención y lo abrí, normalmente no lo hago cuando no reconozco la dirección de quien me envía el correo, sin embargo, lo abrí e inmediatamente se activa el antivirus, me dice que es un archivo de JPG que no implica, no tiene virus, lo abro y era una presentación muy bonita de unas conferencias, ya no recuerdo ni el tema, pero me llamaba mucho la atención que no podía yo identificar quién me lo estaba mandando, tanto el tema, como supuestamente la dirección eran la misma, decía invitación a foro, pero luego de ver y de checar las fechas y de qué se iba a tratar, hasta abajo venía una leyenda que decía: "Este correo no es publicidad comercial, por lo tanto, no constituye Spam y es único y exclusivo y no se le van a seguir generando o mandando este tipo de correos".

Entonces, me llamó muchísimo la atención por dos situaciones: Primera, ¿de dónde tomaron mi dirección de correo electrónico?; segunda, ¿quién me lo mandó?; y, tercera, si esa leyenda efectivamente podríamos considerar que eso no es Spam.

Del contenido del mensaje, uno de los organizadores decía que era el ITESO, el Instituto Tecnológico de Estudios Superiores de Occidente. Entonces quiero suponer que por allí venía la pista de dónde me mandaron esa información. Pero no encontré yo ninguna dirección y esa leyenda que me llamó mucho la atención.

Ponente: Alfredo Reyes Krafft.

Te voy a contestar en dos planos: En un primer plano como abogado y en ese contexto lo que quiero preguntarte es, seguramente tú, al momento de contratar inicialmente el servicio de Yahoo, seguramente leíste el contrato y al momento de leer el contrato pusiste tus datos y definiste un compromiso, hay un acuerdo de voluntades.

Y dentro del apartado o algunos apartados de este contrato, específicamente se establece la posibilidad de que el propio Yahoo o terceros que con él contraten, puedan enviarte publicidad o asuntos en ese contexto. Esa es una parte.

Y dentro de ese contexto habría que verlo, si nos vamos a un estricto purismo.

Dos. Hay un error grave porque no sigue lo relativo o lo que establece la Ley Federal de Protección al Consumidor, en relación al envío de datos. Debe de identificar quién es el que está generando el envío.

Y esa leyenda que dice al final, pues la verdad es que no tiene mucho sentido, cuando menos en lo que es la normativa mexicana, de inicio.

Ahora, ¿a qué quiero llegar? Es importante el esquema de Spam. Dentro del contexto de Spam queda claro, es un riesgo, es un vicio muy grande, pero ninguna legislación va acabar con el Spam, ¿para qué nos hacemos patos?

Es decir, por más que queramos hacer una legislación restrictiva y prohibir el uso en un país en particular el Spam, pues lo que va pasar es que probablemente las empresas que generan mercadotecnia, que pagan impuestos y que lo hacen de acuerdo con la ley, no lo van a poder seguir haciendo, porque va a haber un control y va a haber una restricción muy objetiva, por parte de la propia legislación.

¿Pero tú crees que dejarías de recibir por ello esos mensajes? No. Los vas a recibir y van a partir, pues yo no sé si China o de alguna otra entidad.

Entonces, ¿qué es lo que tenemos que hacer?

Establecer esfuerzos muy grandes, en un plano internacional. Estoy completamente de acuerdo que es necesario contar con una legislación *ad hoc*, pero tenemos que hacerla congruente con

la propia industria: Uno, Yahoo o el prestador de servicios de Internet no necesariamente es el malo contigo. Y en relación con ese punto debemos de adecuar perfectamente bien qué es a lo que nos referimos por Spam, tomar una definición muy clara y muy precisa al respecto.

Porque la distinción entre Spam y lo que sería mercadotecnia directa es muy pequeña.

Ponente: Jesús Rubí Navarrete.

Me alegro de la pregunta y además de que tengamos debate, porque algún matiz discrepante vamos a tener en la propia mesa.

Efectivamente, en el entorno europeo este tipo de comunicación sólo es posible con un consentimiento previo y expreso.

Y además hay un problema adicional, que es que aunque uno celebre un contrato legítimamente con una empresa que le provee de un servicio, en este contrato lo que no es posible es incluir cláusulas vinculantes, como las relativas a la cesión de datos a terceros o la utilización para fines indeterminados, como es la publicidad o la promoción comercial, que se puede referir a cualquier tipo de actividad, de forma que pasen a formar parte del contenido esencial de ese contrato.

Si ese contrato es la prestación de un determinado servicio a la sociedad de la información, ¿qué tiene que ver con el objeto de ese contrato el compromiso ineludible de siempre y en todo caso tener que asumir la posibilidad de que se reciba publicidad propia o de terceros?

Esto es contrario al principio de calidad de datos y es contrario al principio de finalidad.

Y, en el ámbito en el que trabajamos cabe la posibilidad de revocar ese tipo de cláusulas y, en su caso, esto ya no es una cuestión de protección de datos, de llevar a los tribunales hasta qué punto son congruentes con la finalidad del contrato.

Y el hecho de que se produzca, creo que no se puede comparar a la hora de hacer valoraciones en esta materia, el hecho de que haya tratamientos ilícitos con las empresas que tratan de realizar tratamientos lícitos.

No se puede justificar que las empresas que quieren realizar tratamientos lícitos tengan un margen de maniobra superior, porque sino, en todo caso, recibiremos tratamientos ilícitos de la información. Y como da lo mismo porque los vamos a retribuir igual, pues ampliemos el campo de trabajo o reduzcamos el sistema de garantías cuando se pretende hacer un tratamiento ilícito.

Es verdad que hay que buscar una situación equilibrada, pero ese equilibrio no puede tener como punto de referencia la conducta de los que actúan ilegalmente.

Y en lo que se refiere a la leyenda, efectivamente es necesario delimitar qué es Spam. En la legislación de la Unión Europea el Spam se articula como una comunicación de carácter comercial directo o indirecto.

Probablemente esta promoción que usted recibió, desde el punto de vista de esa normativa tendría que ser considerado Spam, auque el que la emite voluntaria o directamente por sí mismo asegure que no lo es.

Ponente: Katitza Rodríguez Pereda.

Yo quisiera dar una sugerencia como consumidor o ciudadano mexicano.

¿Actualmente se están discutiendo proyectos de ley en tu país en México sobre este tema?

Sería bueno que tomen conciencia para que se incluya el conocimiento previo informado que tal vez algunos sectores como la industria no están interesados en preservar en la ley, que todo el mundo nos involucremos y que también que seamos conscientes que en casi todas las transacciones que realizamos día a día depositamos y soltamos nuestros datos personales que pueden ser utilizados e

incorporados en una base de datos e interconectados con otras bases de datos.

Muchas veces el tratamiento de datos personales es invisible al ciudadano, el ciudadano no sabe que ha sido marginado. Uno va a una entrevista de trabajo y te dicen no, no te contrato. Y el empleador tiene toda una base de datos y por ahí ha visto tu récord médico y a raíz de eso ha tomado una decisión de no contratarte.

Tú nunca te vas a enterar porque eso a veces es invisible al ciudadano. Entonces hay que ser conscientes y responsables en todo momento que uno entrega o llena una forma, una ficha, que rellena sus datos con su nombre, teléfono y pensar si efectivamente esos datos son importantes para el servicio que está contratando o le están pidiendo información adicional. Eso es todo.

Pregunta: Alejandro Coto. TEC de Monterrey.

Yo tengo un par de reflexiones que quiero hacer junto con la mesa y, con todo respeto que se merecen, pero yo siento que el tema de Internet en estos últimos 20 años se ha venido autorregulando y el Spam, se va a autorregular tarde o temprano. Y yo quisiera observar que en lo personal, Alejandro Cota, no agrede un Spam mis datos personales, al menos de que haya dado mi dirección de correo, pero soy muy libre de cambiarlo cuantas veces quiera y de cambiarme de proveedor.

Sin embargo sí me extraña y me llama la atención que no estemos cuidando el hecho de la identidad. Uno de los crímenes más fuertes que hay al día de hoy es el robo de identidad y eso sí está agrediendo mis datos personales, y el robo de la identidad no se debe a quién le di o no le di mis datos, si no se debe a cuál es el nivel de seguridad que les estamos solicitando nosotros como sociedad o nosotros como esta red que se está formando, a las dependencias gubernamentales o todas estas organizaciones a las cuales nosotros les damos la información.

Hay organizaciones internacionales en el área de Estados Unidos o ITSEC en el área de Europa en donde sí marca niveles de seguridad de los sistemas de información.

Entonces a mí me gustaría saber qué es lo que opina la mesa al respeto, porque yo sí esperaría que la mesa estuviera preocupada por ver cuáles son las medidas de seguridad que estaríamos solicitándole a las organizaciones que posean estas bases de datos, porque creo que es inevitable que las tenga.

Hoy, después del terrorismo que estamos viendo en el mundo, la identidad es fundamental.

Cuando yo llego a un aeropuerto y casi me desvisten y me piden mi pasaporte y revisan que sea yo quien digo ser, me da seguridad de subirme al avión al que me voy a subir, de lo contrario me daría miedo hacerlo. Sin embargo, qué tanto está agrediendo realmente mis datos personales en contra de la seguridad que todos queremos vivir.

Entonces, vuelvo a plantearlo. ¿Cómo vamos a hacer para que estas organizaciones que poseen mis datos personales realmente tengan niveles de seguridad de los más altos?

Hoy en día los sistemas de identidad de los gobiernos no se preocupan por estos niveles de seguridad.

En México estamos viviendo un proceso, que no sé si se va a llevar a cabo o no. Hacienda es precursora en esto, que era la cédula de identidad para el país.

Sin embargo el nivel de seguridad que estaban planteando en sus estándares era nulo. Nada más decían que hubiera un nivel de seguridad, un estándar internacional, cuando es considerado por Garner Group y por todas las grandes empresas que se dedican a investigar estos rollos, que el nivel de seguridad debería de ser un ITSEC E6, que es el nivel más alto al día de hoy en seguridad. Y esto no está casado con ninguna tecnología.

Entonces, dejo mi preocupación en la mesa.

Moderador: Loretta Ortiz. Directora del Departamento Jurídico de la Universidad Iberoamericana –UIA–México.

Turno la pregunta al que la quiera contestar, pero sí quisiera hacer un brevísimo comentario.

La cuestión del terrorismo, que se acaba de mencionar, ese es el gran conflicto que me da la impresión de que no nos hemos concientizado y que sí va a hacer falta por parte de la sociedad civil, académicos, universidades, y nosotros los abogados también, que hagamos énfasis en el límite que debe de haber precisamente entre lo que es la cooperación judicial para efectos de combatir el terrorismo, el narcotráfico, lavado de dinero, tráfico de personas, tráfico de emigrantes, etcétera, y el respeto a lo que son los derechos humanos de los individuos, porque so pretexto de proteger precisamente ciertos intereses, la verdad es que se alude en la exposición de motivos de estas convenciones internacionales; por ejemplo la de Delincuencia Organizada, que los Estados han perdido control y autoridad, y que entonces la única manera es convencer a los que llaman arrepentidos, que son los que finalmente forman parte del grupo, que son narcotraficantes, o en fin, cambiarles su identidad, darles una vida distinta, ahí está toda la temática.

Y ya con eso gozan de impunidad y finalmente pueden combatir con los datos que les dan al resto de los integrantes del grupo, ya se habla del grupo delictivo. En estas situaciones no hay respeto, jamás se alude en esta Convención Internacional del respeto a la privacidad.

El secreto bancario, expresamente se dice: No opera para esos efectos. Ya con eso uno se puede imaginar que no hay mucha protección ante la cual argumentar frente a precisamente esos esfuerzos internacionales en materia penal, sobre todo terrorismo y narcotráfico, que hacen de lado totalmente los derechos de la persona humana.

Yo me acuerdo que en un foro de discusión se presentó la iniciativa del Presidente, en materia penal, precisamente se distinguían dos tipos de individuos: los que cometen delitos graves y los que no. Los graves no gozan de ningún derecho, se permite la denuncia anónima. Obviamente no se le informa cuál es la causa de la denuncia, vemos que goza del derecho de la presunción de inocencia, en fin, no hay derecho a la privacidad, exactamente igual que en la época de la Inquisición, más o menos ahí podemos ubicar a los que suponen o presuponen que son delincuentes.

Sí hay que tener claro que en estos momentos de presentarse una iniciativa por el buen manejo de los datos personales hay que tomar en cuenta que además del buen manejo y los otros objetivos que se tengan, que es mejorar el comercio internacional, el combate a narcotráfico, la transparencia, etc., finalmente las normas jurídicas están destinadas para gobernar a individuos, a personas y no a instituciones, bueno, obviamente instituciones, pero el principal gobernado, objeto de la norma son individuos y si no se van a respetar sus derechos humanos las cosas no andan bien.

Ponente: Alfredo Reyes Krafft.

Yo quisiera nada más comentar una cosa muy pequeña y es en relación al tema que tú planteaste, es decir, estás hablando de robo de identidad, en dónde va a constar esta identidad, es decir, hoy por hoy una identidad puede constar en una credencial que me puede emitir una autoridad y si yo robo esa credencial o la falsifico, pues de alguna manera estoy usurpando tu identidad.

También esa identidad puede constar en un dato, en un dato pero no necesariamente todos los datos constituyen una identidad y yo creo que aquí habría que hacer un cierto distingo, obviamente es muy importante tipificar como delito, pero no todos los datos que puedo tener referidos a ti van a constituir tu identidad.

Y tercero, otro medio para poder identificarte o para poder definir tu identidad es a través de un esquema biométrico, es decir, conocer que tú eres tú a raíz de la aplicación de una huella digital o el iris de tu ojo.

El problema que existe en la práctica en relación con esos elementos es que no existe un estándar hoy por hoy en la materia.

Entonces, mi huella digital a final de cuentas se va a traducir en un dato, en un uno o cero, y en ese sentido, pues, corre el riesgo de que pudiera ser apropiado por un tercero e interactuar en mi nombre.

Entonces, obviamente se debe de interactuar, se deben de establecer penas muy fuertes en ese sentido y se deben establecer criterios, claro, de custodia de todos aquellos datos que puedan servir para identificarme, que acrediten de alguna manera directa o indirecta la identidad.

Completamente de acuerdo contigo.

Ponente: Jesús Rubí Navarrete.

Yo le diría en lo que se refiere a la parte de seguridad. Efectivamente hay que buscar equilibrios en todos los casos, por ejemplo, en el caso de las investigaciones criminales, nosotros hemos tenido atentados tremendos en Madrid que han implicado su resolución, el tratamiento de determinados tipos de datos de comunicaciones electrónicas.

Pero ese equilibrio se puede contar, se puede encontrar, hemos estado analizado qué tipos de datos son los necesarios para poder realizar ese tipo de investigaciones, cómo no es necesario acceder al contenido de las comunicaciones para hacer ese tipo de investigaciones, hemos estado analizando para qué finalidades se pueden permitir esos accesos, porque no es lo mismo permitir acceso a determinada información para perseguir el terrorismo, que poder utilizar esa información, pongamos por caso absurdo, para perseguir sanciones de tráfico.

Entonces, aunque todos sean fines de interés público, hay que acotar las finalidades y hay que establecer plazos máximos, en su caso, del tratamiento de esta información.

¿Y a qué lleva todo esto? Pues a que desde el punto de vista de la seguridad es imprescindible que las medidas de seguridad sean de un nivel elevado, por dos motivos: Primero, porque esta una información muy sensible, inclusive desde el punto de vista de quien la utiliza para hacer investigaciones criminales y si se producen alteraciones en esa información, las propias investigaciones criminales pueden fracasar. Por tanto, hay que mantener íntegra la información y eso exige un nivel de seguridad elevado.

Y, en segundo lugar, porque hay que controlar adecuadamente quiénes son los usuarios habilitados para acceder a esa información y poder evaluar e impedir que accedan, por ejemplo, nuevas ideas sobre el terrorismo, usuarios no autorizados, y ellos nos vuelva a llevar a la necesidad de que las medidas de seguridad sean de un nivel elevado.

No se pueden poner en marcha proyectos que implican un riesgo desde muchos puntos de vista, no sólo desde la protección de datos personales para el tratamiento de la información, si no se está dispuesto a asumir que tienen que tener unas medidas de seguridad técnica y organizativa de un nivel elevado.

Desarrollos Normativos y Globalización

Mesa 3:

Moderador: Isidro Cisneros. Profesor Investigador de la Facultad Latinoamericana de Ciencias Sociales –FLACSO– México.

Está tarde nos acompañarán el doctor Juan Antonio Travieso, Director Nacional de Protección de Datos Personales de Argentina; David Banisar, Director Adjunto de Privacy Internacional del Reino Unido; Jesús Orta Martínez, Director General Adjunto de Operación de la Secretaría de Economía de México; Juan Pablo Pampillo Baliño, Director Jurídico de IBM de México y Roberto Andrade Martínez, Gerente de Contratos de Telefónica Móviles-México.

Conferencia Magistral: Juan Antonio Travieso.

Ante todo voy a agradecer, como es habitual, a los organizadores, por supuesto a María Marván con esa fuerza, con ese talento; a los amigos de España, a José Luis, a Jesús, siempre cuando uno tiene amigos les dice por su nombre. Así que es la forma habitual de poder tratar a esos queridos amigos, a José también, a todos los que siempre luchan y realmente están en una cruzada muy importante.

Hoy me voy a referir a dos temas que aparentemente son absolutamente difíciles de poder unir que son: los desarrollos normativos y la globalización, en realidad voy a invertir los términos. Vamos a hablar primero de la globalización, que es el gran tema y que tiene que ver con la reunión que en este momento se está realizando en la ciudad de Mar del Plata en la Argentina, donde precisamente los países de América estamos discutiendo el esquema con relación a América y estamos pidiendo nuevas condiciones que tienen que ver fundamentalmente con los subsidios.

Hace pocos años que estamos percibiendo un cambio en la sociedad nacional e internacional.

Hay un terremoto que sacude al Planeta: terminó la guerra fría, estamos en la guerra caliente de la economía. Estamos en plena época de la globalización y sucede que hace pocos días leía un artículo en que las situaciones que esta globalización hace que los viejos estén más jóvenes que nunca, no es mi caso, y los jóvenes son más viejos que nunca.

En los unos se perciben las alegrarías chispeantes de la biotecnología. En los otros, la prudencia y el cálculo anticipado; de responsabilidades, nada, vivimos la vida en tiempo real, no hay tiempo para

otra cosa. Esta situación se denomina hoy tecnonihilismo en lo que estamos viviendo y lo que tiene que ver básicamente con la globalización.

Y la herencia del nihilismo del siglo pasado en las sociedades tecnológicas del nuestro no es ya un nihilismo hacia atrás, sino hacia delante. Antes indicaba el colapso del pasado, ahora es el colapso del futuro.

Es decir, la globalización se presenta entonces con unos enormes desafíos y con unos enormes riesgos. Nos encontramos con verdaderas Apocalipsis, las dos variantes más temidas: la amenaza terrorista y verdaderamente el futuro como desilusión.

Esto tendría que ver parcialmente con la protección de datos, porque la protección de datos en la globalización es un detalle más, es el tema de la soberanía, es decir, cómo va cambiando y cómo los nuevos ejes en el Estado nación en la actualidad pueden entenderse en una forma distinta en los que los datos personales van a jugar un rol protagónico.

El eje económico, el eje tecnológico, el eje informático, dinero electrónico, capital especulativo y el eje de las comunicaciones, fundamentalmente el de Internet. Esto plantea nuevos paradigmas con la posibilidad de redefinir al Estado.

He escrito hace unos años en que la forma de poder encontrarle la solución a todas estas cuestiones es a través de plantear la globalización desde un criterio pentagonal. El criterio pentagonal, no quisiera ser calificado como un intelectual burocratizado.

Recuerdo que decía Ortega que *la tarea del intelectual siempre es tomarle el pulso a su tiempo*.

Y esta globalización en la que los ricos cada vez se llevan más y los pobres menos; la clase media se va vaciando lentamente, se está generando una inestabilidad, quizá un proceso de discontinuidades en la que la cuestión social no puede soslayarse cuando un 20 por ciento se lleva el 80 por ciento de los ingresos.

Y por eso el *Plan A*, para entender la globalización, es entenderla desde un criterio pentagonal que consistiría en un enfoque crucial de la pobreza, el empleo, la distribución de la riqueza, la no contaminación que tiene que ver con los desastres ecológicos y el desarrollo del concepto de ciudadanía el que nos subimos acá entonces con la protección de datos.

¿Qué es la ciudadanía? En realidad es la posibilidad que existe desde mediados del siglo XX en la cual se presenta la condición de los sujetos para pasar a considerarse como una capacidad para el ejercicio de los derechos.

Un ciudadano o una ciudadana construyen su ciudadanía en su relación con el Estado responsable de garantizar ese ejercicio.

Con sus políticas públicas el Estado fortalece o debilita la ciudadanía de sus habitantes, promoviendo o no el respeto, la accesibilidad, la difusión, la participación y el control de sus derechos que también implica, por supuesto, la protección de datos personales.

Lo que sucede en esta época, sobre todo en América Latina, es que nos encontramos con una situación enormemente dispar y complicada. Pero más allá de eso, también, con relación a la información y la informatización nos encontramos en que hay una nueva forma de interpretar el mundo. Hoy el tema es el mundo, es el mensaje, ahora el medio es un *byte*, está comprimido, está sintetizado, excede el panorama de lo que puede ser un *diario*. Ya un diario es una información hasta pretérita.

No hay una transmisión diaria, sino que la transmisión es en segundos. No hay tiempo para la reflexión. Es la época del tiempo real, pero hay algo más, porque asimismo ante el nuevo esquema tiene relación con el esquema de las relaciones de producción.

En la sociedad industrial todo se medía a través de relaciones de producción y la atención entre capitalistas y trabajadores. De ahí salían los ganadores y perdedores.

En el sistema de información, lo que impacta es la exclusión y no la explicitación. El tema no es si uno es o no explotado, sino el problema es si uno tiene acceso al flujo de información o no.

Aquellos que no acceden al flujo de información son los nuevos desarraigados del siglo XXI y los futuros desaparecidos del siglo XXII, los incluidos son los que se conocen cara a cara en la ciudad global aunque no se hayan visto nunca.

Ante esta situación, para poder entender una protección de datos que atienda esa realidad se debe tener en cuenta lo que algunos autores han llamado las tres nuevas lógicas rectoras.

La primera, que lo nacional es desplazado por lo global, y eso sucede en cuanto aspectos financieros y tecnológicos como los que me referí al principio cuando dije acerca de los ejes. Y en el plano político las instituciones supranacionales que sustituyen a las instituciones del Estado nación.

La segunda es la lógica de la información, que sustituye a la lógica industrial.

La tercera es el desplazamiento de lo social por lo cultural, como se trata de una sociedad de flujos, los flujos están compuestos de bienes simbólicos o culturales con una declinación intensa de las instituciones, tales como las iglesias y los partidos políticos.

Lo que importa no es la relación dentro de la institución, sino la relación interpersonal y aquí, entonces, se produce el cambio de paradigma, se materializa un nuevo paradigma. En realidad, el nuevo paradigma es el derecho a estar a solas en compañía de los demás, una sociedad con autoridad que en su expresión más extrema se presenta en la persona conectada por Internet en un *Chat* sin rostro alguno, compartiendo todos sus datos incluso, su propia identidad con un gran hermano que lo vigila todo.

También verificamos que la protección de datos personales tiene un desarrollo de décadas y se verifica dentro de un amplio cambio de paradigmas de los cuales esta reunión es la expresión más cabal.

En consecuencia, entonces, lo que importa es que hay un enfoque alternativo que tiene que ver con esta nueva sociedad del siglo XXI en la cual le tenemos que agregar esa ecología informática, la protección de datos es lo que le agrega ese plus para la ecología informática.

Entonces, la clave sería incentivar el flujo de datos y la información, pero al mismo tiempo concienciar, como se está haciendo aquí, acerca de la protección de los datos personales.

La prueba es encontrarles la solución a todos estos modelos y sabemos perfectamente que hay cuatro modelos fundamentales para la protección de la privacidad.

El primero es el de las leyes de marcos, en el que una ley comprende la captación, el uso y la diseminación de información personal de los sectores públicos y privados, este es el esquema preferido por Argentina y la mayor parte de los estados europeos, otros países como Canadá y Australia usan un modelo de corregulación mediante el cual la industria adopta reglas para la protección de datos personales que luego son controladas por la propia industria y los organismos de control.

El segundo modelo es aquel que evita la sanción de una norma general y propicia reglas sectoriales, como es el caso de Estados Unidos.

Cabe resaltar que este es un sistema que implica introducir normativas para lograr estándares de protección.

El tercer sistema es el de autorregulación.

Yo creo que este primer enfoque, que es el enfoque general y el marco conceptual, desearía participar con ustedes de algunas experiencias que he vivido en mi función como Director Nacional de Protección de Datos Personales.

En primer lugar, debo decir que la Argentina, igual que en todos los países del área, la única ley, la ley que más se cumple, la ley que más se obedece y se cumple es la ley de gravedad.

Y fundamentalmente la clave de todos, es una clave casi colonial, que es: la ley manda, pero no la cumplo. Por eso, el otro día cuando entregué los certificados de inscripción, uno a uno fui entregando a los distintos actores que habían recibido y que habían sido calificados como para poder tener su certificado, cada uno de ellos me dijo: gracias.

Yo realmente no pude reprimir la emoción porque sentí, gracias por qué, porque lo que están haciendo ustedes es simplemente cumpliendo con la ley.

En un lugar donde no se cumple ninguna ley, como en todos nuestros países, yo no quiero hacer autocrítica de la Argentina, la clave nuestra fundamental es el irrestricto cumplimiento de la ley y fundamentalmente no solamente tenemos eso, sino que además, le agregamos otros problemas, en algunos países nuestros tenemos regímenes federales con distintas autonomías, donde le vamos agregando más inconvenientes o más problemas, más condimento a esta ensalada.

Y ahí se produce esa interacción mutua, en donde es necesario atender al marco conceptual, pero también atender a la transversalidad de los temas.

Yo creo que más que una conferencia el mismo programa que ilustra la realización de este seminario, de este Encuentro, es la expresión más clara, más patente de lo que es una globalización, una intersección y una transversalidad de cumplimiento de acciones.

Les digo básicamente que he recibido la influencia y no tengo ningún problema en decirlo, la influencia muy benéfica de la legislación española, en especial mi país ha recibido la influencia en cuanto a la política y ejercicio de la protección de datos, hemos recibido la influencia también de casi toda Europa y también participamos con muchos de los criterios de protección de Estados Unidos, en cuanto a la protección del consumidor.

Debo decir también que en todos los momentos, cuando se organizó, cuando se está organizando lo que yo llamo los cuatro motores: motor número uno, el Registro Nacional de Base de Datos Privadas. He recibido la influencia benéfica, los aportes, los consejos de las distintas autoridades, en especial de la autoridad española, que siempre nos ha acompañado prácticamente como una sombra de nuestra dirección, una sombra benéfica, no una sombra mala.

Debo decir también que tanto en las sanciones, fíjense ustedes, a veces es importante copiar, pero no copiar del todo. El primer acto de mi oficina fue dictar la norma sobre las sanciones y la copié, porque a veces dicen “es mejor no inventar la pólvora”, pero a veces es necesario inventar la pólvora, aunque uno se queme un poco.

Y precisamente en la primera parte apliqué esa norma de sanciones y hace pocos días firmé una nueva norma de sanciones mucho más elástica, mucho más práctica, mucho más funcional.

Estoy al borde de cambiar el procedimiento, hacer un procedimiento que asegure los derechos para las dos partes.

Si ustedes me permiten, les voy a dar un consejo a los que no tienen ley: Traten de hacer, lo hago con toda humildad, traten de hacer de que la ley no sea el objeto de una expresión autoritaria, de un sector o de un grupo de iluminados, sino que la ley o las disposiciones sean exclusivamente el objeto y el motivo de una discusión razonada entre distintos sectores en pugna.

Incluso es muy bueno aquellos que no opinan como nosotros; nos facilitan, nos dan ideas, nos aportan creatividad, nos aportan modernización.

La crítica es fundamental y para esto cuento con el bagaje de ser un profesor universitario, en donde la crítica para nosotros es fundamental y eso, entonces, me permite poder actuar en un marco de formación participada de normas.

Así lo hice cuando fui Jefe de Gabinete de la Secretaría de Justicia y se dictó el primer decreto. Todo el mundo participó, todo el mundo aportó, así lo estoy haciendo ahora con las normas de seguridad, que incluso las he metabolizado a distintos sectores y, por supuesto, también a la autoridad española, que me dio bastantes consejos sobre la forma de implementarla.

Y al mismo tiempo también ejercitamos la globalización. ¿Cómo? La globalización empieza por casa, empieza con los cuatro motores; sigue en las provincias, en las provincias conectadas. Tenemos 400 puntos de denuncias y reclamos para derechos de supresión, de rectificación de datos, en todas las oficinas que pertenecen a defensa del consumidor. Se ejecutan esas denuncias y esas denuncias pasan a nuestra oficina, para que sean también analizadas.

Otro consejo que me permito darles con toda humildad es: Utilicemos las acciones del Estado en forma eficiente. No nos quedemos directamente en que la oficina es un círculo cerrado, un castillo de marfil, utilicemos todas las distintas acciones.

Fíjense ustedes, ahora viene, por ejemplo, el tema de las inspecciones. ¿Cuántos inspectores hay que tener en la calle?, en un país en que la única ley que cree y que se aplica es la ley de gravedad. Ustedes dirán: cuatro mil. Sí, efectivamente, hay que tener cuatro mil inspectores.

¿Y cuánto cuestan cuatro mil inspectores? Bueno, en este momento estamos efectuando un acuerdo con distintos sectores de la sociedad, para que tengamos inspectores que actúen para nosotros y que nos digan si está inscrito o no inscrito que es la primera parte, para el cumplimiento de estos temas.

Pero la globalización no termina allí, sigue en el MERCOSUR. Tenemos que influir en los ámbitos cercanos con nuestros vecinos.

Todos ustedes son vecinos, todos ustedes son compatriotas de la gran patria americana. Pero también tenemos que incentivar en los ámbitos en los que estamos desarrollando la integración como, por ejemplo, en el MERCOSUR, criterios de políticas, criterios de estructura en cuanto a la protección de datos.

En este sentido estamos trabajando activamente en el *Subgrupo de Trabajo número 13 de comercio electrónico*, con un texto que al principio fue el texto argentino y hoy en día ese texto es brasileño-argentino, hemos incluido un nuevo eje en el esquema, que me permite agregar, a nivel internacional, en cuanto a nuestro sistema de MERCOSUR y de integración local, agregar fundamentalmente transversalidad y calidad institucional.

Porque fundamentalmente, en ese sentido, nosotros hemos tratado de establecer cuatro puntos fundamentales, que son el tema de los datos sensibles. Y en datos sensibles no hemos tenido la tentación directa que es el de aplicar como una autoridad de control, sino conjugar, tener en cuenta que atrás de cada dato sensible no solamente estamos protegiendo a una persona, sino que también estamos protegiendo industrias que son muy importantes para el desarrollo de nuestra economía. Y del desarrollo de nuevos medicamentos. Es decir, tenemos que conjugar ese sistema mediante el cual no provoquemos el síndrome del elefante en un bazar, que por el hecho de controlar rompemos todo.

Siempre recuerdo consejos de autoridades de control que me decían no hay que ser fundamentalista en materia de datos personales, hay que ser constructivista, hay que construir, hay que trabajar.

Hoy escuché una excelente conferencia acerca de transferencia internacional sobre la cuestión en la Unión Europea y en el mercado interno, estamos aplicando las mismas reglas copiadas, ahí sí hacemos marketing de la Unión Europea, copiamos incluso las mismas fórmulas para transferencia internacional idénticas, no inventamos nada, no inventamos la pólvora porque la pólvora ya está inventada, muy simple, y además esto genera negocios, genera desarrollo, genera crecimiento y creatividad.

En cuanto marketing directo. Hace pocos días estuve en Atlanta en un seminario, en un congreso de marketing directo. Yo realmente se los digo desde mi humilde punto de vista, no conocía que era tan importante el marketing directo, marketing directo es el 10 por ciento de la economía norteamericana, mil 230 millones de millones de dólares; la economía argentina son 150 mil millones de dólares.

Y el congreso éste estaba integrado por 11 mil personas. Es decir, 11 mil personas donde uno le está diciendo a ellos, ojo con los datos personales, no molesten a la gente con el telemarketing. Recuerden ustedes que con el telemarketing ya hay anotadas cien millones de personas en el no me llamen.

Es decir, hay un esquema en donde también podemos ser útiles, al mismo tiempo que somos útiles y que estamos agregando creatividad. Estamos, también, no solamente protegiendo a las personas, que es nuestra obligación principal, sino protegiendo el trabajo, la actividad de nuestros compatriotas y la creación de riqueza y, por supuesto, la información crediticia que es el otro sector que es en donde estamos precisamente desarrollando una acción de protección a las personas y de mantenimiento de criterios lógicos.

Debo decir que les agradezco mucho poder haber hecho esta combinación tan difícil entre la globalización y el desarrollo normativo. Disculpen que he hablado de mi persona, pero realmente es lo que más conozco o lo que más desconozco, pero lo he hecho precisamente con el ánimo de poder construir o de aportar algún tipo de solución.

No los dejen solos, un último consejito si me permiten, no dejen solos a los legisladores, los legisladores no son dioses. Mañana cualquiera de nosotros podemos ser legisladores y necesitamos el aporte de todos y cada uno; llévenles aportes, llévenles soluciones, porque el legislador está esperando estas cuestiones.

Moderador: Isidro Cisneros. Profesor Investigador de la Facultad Latinoamericana de Ciencias Sociales –FLACSO– México.

Muchas gracias al doctor Juan Antonio Travieso, quien además es un defensor y un estudioso de los derechos humanos, lo cual hace doblemente grata su presencia esta tarde.

Ahora pasaremos a escuchar al profesor David Banisar. Es Director del Proyecto para la Libertad de Información, investigador visitante en la Facultad de Derecho de la Universidad de Linz en el Reino Unido y Director del Proyecto para la Libertad de Información de Privacy International en Londres; antes, fue investigador de política en el Open Society Institute e investigador de la Universidad de Harvard; en la actualidad hace investigación y escribe sobre desarrollos globales en relación a información y la privacidad; ha trabajo en el campo de la política de información por 14 años y es autor de numerosos libros de estudio relativos al acceso a la información y artículos sobre libertad de información, libertad de expresión y privacidad.

Ponente: David Banisar. (Traducción simultánea)

Vamos a ver los conflictos que existen entre Estados Unidos y la Unión Europea en cuanto a cuáles son los que se van a adoptar en todo el mundo.

Tal vez sea exagerar un poco que se ha extendido la influencia de parte de Estados Unidos y la Unión Europea sobre qué modelo se debe adoptar.

Se puede ver esta batalla en muchas sedes distintas, se puede ver a nivel nacional en un país como México, porque ahí se proponen muchas cosas. Hay delegaciones de ambas jurisdicciones que hacen visitas, presentan sus puntos de vista, hay organizaciones y hay compañías de estas jurisdicciones que presentan sus puntos de vista y también lo veo en acuerdos de libre comercio internacionales, y también otras facetas de la globalización, en cosas como lo que es el desarrollo de los principios de la APEC, y es importante ver a los países que no tienen todavía leyes, hay que ver cuáles serían las sanciones o cómo están construyendo la democracia.

Hay muchas presiones y muchos factores que influyen aquí. Entonces voy a hablar del contraste que hay entre los dos modelos.

Creo que el contraste más importante, y esto hablando de que yo estudié abogacía en Estados Unidos y puedo ver a ambos lados.

Esto es realmente el contraste entre lo que es más importante, el respeto por los derechos humanos o el respeto por los derechos comerciales.

Ya ha habido mucha discusión sobre Europa, en una primera sesión. Vamos a ponerlo en contexto, en Europa se respeta mucho lo que son los derechos humanos y esto incluye casi todo el continente con algunas pequeñas excepciones.

La Convención Europea de los Derechos Humanos, que ahora ya está en vigor y que es aplicable en todos los países de la Unión Europea. Y el artículo ocho da mucha protección a la privacidad y obviamente esto ha estado en vigor en el Tribunal Europeo de Derechos Humanos, incluyendo el reconocimiento por parte de este Tribunal, de que hay derechos de protección y restricciones sobre la difusión de información, las formas de acceso y los derechos de corrección.

No solamente es un asunto de estatutos, sino de derechos constitucionales que se han adoptado más o menos en 45 países en sus sistemas legales.

Y en comparación con esto en los Estados Unidos la Suprema Corte, desafortunadamente, solamente tiene o ha reconocido un derecho muy limitado a la privacidad y han existido algunos casos especiales en relación con los registros médicos, pero la mayor parte de los datos los tienen terceros, pueden ser datos financieros, pueden ser datos de telecomunicaciones, registros de telecomunicaciones como los registros del teléfono, y la Suprema Corte no ha querido dar un reconocimiento formal con el derecho de privacidad, puedo mencionar datos todavía más importantes.

Hay algunos estados en la Unión Americana que ya tienen derechos constitucionales a nivel estatal nada más, pero no llevan el nacional.

El segundo contraste que creo que ya se mencionó es el de la autorregulación contra la ley.

La pregunta, la cuestión aquí es: ¿Si es mejor tener muchos derechos que proteger o basarnos en las empresas con sus reglas internas y las decisiones que toman para proteger esta información? Obviamente ya escuchamos mucho sobre los sistemas y lo voy a extender un poquito más en un momento.

Tal vez ya lo saben, el sistema de Estados Unidos está más enfocado en la autorregulación donde las compañías hacen compromisos o promesas de no revelar la información o solamente la utilizan de manera legítima, pero en general, estos compromisos no solamente incluyen el acceso de algunas personas a esta información o el derecho de corregir información correcta o incorrecta. Y no hay una ley específica que regule esto. Normalmente no se pueden aplicar excepto en casos muy limitados.

Por ejemplo, tenemos una aerolínea, se llama *Jet Blue* y tiene una página Web, ahí ustedes se registran, seleccionan el vuelo que quieren y la

política de privacidad menciona que la información financiera y personal no se comparte con ningún tercero; excepto cuando se descubrió que en realidad sí se estaba transfiriendo esta información al Pentágono, a los militares.

Los militares usaban la compañía para manejar este registro de transferencias y los viajes de los pasajeros, para ver si ésta se podría utilizar en la guerra contra el terrorismo, pero esto no estaba en la política de privacidad, dice que para ningún tercero. Pero le estaban dando esta otra parte sin que nadie lo supiera.

(Se refiere a su presentación en PowerPoint) Es la misma compañía que tomó los datos de *Jet Blue* y compró información adicional de otra empresa que se llama International Action Center que estaba colocando información muy sensible y la daba a las agencias gubernamentales y esto en realidad no seguía la Ley de Privacidad.

Y Action estaba vendiendo, estaba dando información relacionada con datos de niños, el seguro social, ocupaciones, información de los vehículos y todo estaba en esta base de datos gigante.

Lo que se descubrió es que hubo una demanda enorme contra ellos, contra Jet Blue y contra Action, y el Tribunal dijo hace poco que como los individuos no podían salir dañados, entonces no tenían ningún derecho, aunque la promesa que se les había hecho se había violado.

La solución quedó pendiente para terminar de investigar la demanda, y no quisiera saber cómo va a terminar el asunto.

Otra área donde estas promesas no están funcionando muy bien es en la seguridad. El directivo de la Unión Europea requería que la información personal se protegiera, que hubiera algunos medios técnicos administrativos para que no se difundiera esta información de manera accidental o a propósito. Y las políticas de privacidad pueden tender a algo parecido a esto, pero finalmente no hay tanto problema.

En California hay una empresa que ha guardado mucha información y creó puentes para el proceso de información. Había información personal a gran escala, que se pasó sin autorización y era de más de 50 millones de personas. El estado de California indicó que parte de esta información se dio a conocer de manera accidental y la compañía le tenía que decir a esta gente por qué. Esta entidad tiene un gran mercado, y obviamente podría incluir al resto del país.

Mucha de esta difusión fue accidental, desconocida. Por ejemplo, cintas magnéticas que contenían información financiera de los bancos, que se entregaban por camión y simplemente desapareció. Esperemos que solamente la hayan tirado por algún lado, pero no sabemos qué sucedió en realidad.

En algunos casos los *hackers* entraron en los sistemas de cómputo, en otros, algunas personas de adentro utilizaron las contraseñas para accesar la información. La información es un problema importante, en ausencia de un requerimiento legal para hacerlo.

La tercera área de la que quisiera hablar es el asunto de que si tienen una ley o quieren una ley completa y no una ley que solamente cubra un sector, es mejor tener un marco. Obviamente los europeos prefieren un marco más completo y ha sido el enfoque durante 35 años, desde que se empezó a adoptar esta ley. Esto es común en casi todos los países en la Unión Europea y en casi todos los países en Europa, hoy se trata de 40 países que han tomado este sistema completo.

La consecuencia de no tener este sistema es que si solamente tiene una ley sectorial las cosas cambian, la tecnología cambia, y si la tecnología cambia la ley no necesariamente cubrirá la nueva tecnología. Por ejemplo, Estados Unidos con la televisión por cable interactiva está

protegida, pero los registros por Internet no. Se tienen anomalías muy extrañas cuando se hace esta información, dependiendo de quién la tiene y no está protegida. Este es uno de los casos por los que suceden o se dan los fraudes tan seguidos, y en Europa no es tan común tener Spam.

Otro caso que se mencionó es Australia y Canadá, que tienen otras formas de hacerlo, como la combinación de los dos. Tiene algunas cosas positivas, otras que funcionan nada más en Canadá y no ha tenido mucho éxito en Australia, por la falta de aplicación y de autoridad.

Moderador: Isidro Cisneros. Profesor Investigador de la Facultad Latinoamericana de Ciencias Sociales –FLACSO– México.

Tiene la palabra Jesús Orta Martínez, es Director General Adjunto de Operación de la Secretaría de Economía; es licenciado en Economía por el Instituto Tecnológico de Estudios Superiores de Monterrey y maestro en Economía por El Colegio de México.

Ha desempeñado distintos cargos en la Administración Pública Federal y entre sus responsabilidades y funciones actuales se encuentra la de ser Coordinador del Programa para el Desarrollo de la Industria de Software, responsable de la Política Regulatoria y de Fomento del Comercio Electrónico, delegado del Gobierno mexicano ante el Comité de Política de Tecnologías de Información y Comunicaciones de la Organización para la Cooperación y el Desarrollo Económico.

Ponente: Jesús Orta Martínez.

Para la Secretaría de Economía es un foro muy importante y además de mucha actualidad porque, como ustedes saben, en México estamos discutiendo legislación al respecto.

Y yo, naturalmente, siendo representante de la Secretaría de Economía, tengo una perspectiva regulatoria muy identificada con la parte de los flujos de información y su impacto económico.

Déjenme centrarme en un par de cosas que iremos viendo a lo largo de estos 10 minutos.

(Presentación en PowerPoint) Voy a introducir el tema de este panel y decir que globalización en este contexto implica necesariamente un incremento en el tráfico de flujos transfronterizos de datos personales. Para México esto es importante, porque es el país con más tratados comerciales en el mundo, naturalmente el tema de los flujos de datos que son consecuencia o que provienen de relaciones comerciales, es un asunto importante en términos de no impedirlos y, en todo caso de lograr un equilibrio entre lo que es un derecho fundamental, como ya se dijo, es el derecho de privacidad; otro aspecto importante desde el punto de vista económico que es ese flujo fluido, valga la redundancia, de datos transfronterizos.

El grado de sensibilidad respecto al tema de privacidad, hay diferencias entre las regiones, evidentemente para Europa que es una región hipersensible a este tema. Hay países en Asia que no les importa en absoluto el tema y hay países en Latinoamérica en donde no hay conciencia necesariamente o conciencia generalizada del asunto de la privacidad.

Eso también tiene una influencia sobre el enfoque que un país pueda llegar a tener sobre el aspecto de la privacidad. Por cierto yo presido el grupo de comercio electrónico de APEC, y tuve la oportunidad de darme cuenta de este factor, de palparlo muy claramente. O sea, el tema de privacidad o el grado de sensibilidad de ese tema difiere drásticamente entre regiones.

Los enfoques normativos regulatorios son diversos y en ocasiones divergentes; ya se habló del caso de Estados Unidos y la Unión Europea por mencionar uno, que ese es más claro y más relevante tal vez y los esfuerzos multilaterales entonces se han centrado en buscar la convergencia.

Voy a mencionar rápidamente cuáles son algunos de esos esfuerzos multilaterales y naturalmente me estoy enfocando en aquellos

en donde México tiene una presencia por membresía, particularmente la OCDE y ese documento que seguramente todos ustedes conocen, que es como quien dice el padre de todos los documentos junto con naturalmente las disposiciones de la directiva europea al respecto.

APEC, como lo mencioné, acaba de sacar en noviembre del año pasado su marco de privacidad, y México actualmente está involucrado en una negociación a nivel región con Estados Unidos y Canadá en el marco de la Alianza para la Seguridad y Prosperidad de América del Norte (ASPAN), que viene a ser algo así como una especie de transición entre lo que es el TLCAN y lo que se ha llamado en los medios el TLCAN Plus, que es ir más allá de lo que es la relación comercial para ir a una integración de otro tipo, de mayor valor agregado, naturalmente.

Me voy a concentrar en este aspecto de APEC, ¿por qué? Porque es el desarrollo multilateral más nuevo. Y aquí hay un matiz importante, Europa no participa, pero sí participan los países asiáticos y hay que recordar que APEC es el foro multilateral que congrega a las economías más dinámicas en términos de crecimiento económico en el mundo, incluido por supuesto China, pero también Japón y Corea; además el bloque norteamericano: Estados Unidos, México, Canadá, dos países adicionales de Latinoamérica como son Chile y Perú, y en general todos los de la zona de la Cuenca del Pacífico.

Dentro de lo que es el grupo de comercio electrónico de APEC, que fue creado en 1999, a partir de un mandato de los líderes de este foro, tiene como actividades prioritarias protección al consumidor, seguridad cibernética, comercio sin papel, Spam, y por supuesto el tema de la privacidad.

El tema de la privacidad adquiere dentro de este foro, desde hace tres años, un papel fundamental, y no es para nadie un secreto que nuestro vecino del norte fue quien lo empujó; porque como ya se mencionó Estados Unidos al igual que la Unión Europea tienen intereses importantes en términos de quién va a prevalecer en cuanto al enfoque o la aproximación hacia el marco regulatorio, en todo caso, que va a tomar el mundo.

Hablaba al principio de que los esfuerzos multilaterales se han tratado de centrar en la convergencia. ¿Por qué?, porque se ha identificado una divergencia grave que puede tener consecuencias como las que está teniendo el problema de los estándares en lo que son los sistemas de cómputo, es decir, si no vamos hacia estándares que puedan comunicarse entre sí, y aquí el símil sería si vamos hacia marcos regulatorios o enfoques normativos que son divergentes o incompatibles, vamos a tener un problema de otro tipo.

Es decir, en pasar de un marco normativo pensado para un país, pensando hacia adentro, las consecuencias al interactuar, y el tema entonces de la globalización es relevante con otros países, podríamos tener un conflicto importante. Ese conflicto, el caso más claro o el ejemplo más claro de cómo se ha concretado es el de Estados Unidos y el de Europa que ha derivado, como seguramente todos conocen el instrumento en el *Safe Harbor* [1] o el puerto libre o no sé cómo se diga en español eso, pero que a final de cuentas no es más que un parche hacia dos enfoques regulatorios que son distintos, porque en su origen tienen distintas formas de atacar el problema.

Este esfuerzo de APEC busca generar convergencia y naturalmente al estar Estados Unidos dentro de este foro y no Europa, pues ya se imaginaran el sesgo. Se crea un grupo especial, un subgrupo especial, que es el subgrupo de privacidad de información.

Y en general este marco de privacidad de APEC, o el APEC Privacy Framework, que es como se

[1] El safe harbor es el nombre con el que se conoce el protocolo que garantiza un nivel adecuado de seguridad en la protección de datos. Fue el Departamento de Comercio de los Estados Unidos quien creó la lista y es de inscripción voluntaria. Actualmente hay 72 empresas norteamericanas registradas.

llama originalmente y que va a ser publicado oficialmente y distribuido en la próxima Cumbre de Líderes de APEC en noviembre, fue desarrollado tomando evidentemente los principio de la OCDE sobre privacidad y tomando en cuenta disposiciones de la directiva europea.

Tiene como fin los siguientes aspectos: Proteger la información personal, como principio fundamental; pero también, prevenir la creación de barreras innecesarias al flujo transfronterizo de datos.

Y aquí la palabra más importante y más recurrente de este desarrollo multilateral sobre protección de la privacidad es equilibrio, equilibrio entre protección a la privacidad y flujo de datos; fomentar la uniformidad por parte de empresas en los métodos utilizados para la recolección uso y procesamiento de datos personales, y aquí viene una innovación, que es lo que se conoce como "corporate policy rules", que no son más que una especie de reglas a nivel de empresas que tratan de hacer uniforme lo que son estos elementos que son recolección, uso y procesamiento de los datos, y la uniformidad nos puede dar muchas ventajas importantes a la hora de abordar el tema de la protección a la privacidad y naturalmente fomentar los esfuerzos naturales e internacionales para promover y hacer cumplir las disposiciones legales.

Son nueve principios, no me voy a ir sobre ellos, ustedes lo pueden consultar en todo caso en la página ap.org y además va a salir pronto la publicación, pero son nueve[2] principios que abordan de manera holística este problema de la privacidad.

Y en cuanto a la implementación tiene dos anexos que salieron este año, la parte doméstica que es para todas aquellas economías que no cuentan con un marco regulatorio, ya sea específico o sectorial sobre el tema con enfoque o con la idea de darle importancia a la consulta a los sectores involucrados, el diálogo entre sector público y privado para no sesgar ni hacia un lado ni hacia otro en cuanto a los intereses, fomentar la educación y la conciencia del derecho de la privacidad porque, como ya mencioné, muchas economías no tienen ni siquiera esa conciencia.

Y un aspecto que es el de la cooperación internacional y que aborda, digamos, aspectos que tienen que ver con la importancia de que al final del día si tenemos un problema que es de globalización, que es de flujo de datos y así como sucede con el Spam, no se va a poder resolver o a garantizar la protección de datos en la medida en que los países no tengan acuerdos para poder colaborar y cooperar internacionalmente en materia de investigación, como de persecución y de otro tipo de asuntos propios de hacer cumplir las leyes y los marcos legales.

Moderador: Isidro Cisneros. Profesor Investigador de la Facultad Latinoamericana de Ciencias Sociales –FLACSO– México.

A continuación Juan Pablo Pampillo Baliño. Director Jurídico de IBM de México, quien es abogado egresado con honores de la Escuela Libre de Derecho, diplomado de estudios avanzados equivalentes a maestría, egresado con honores de la Universidad Complutense de Madrid con estudios completos de doctorado.

Ponente: Juan Pablo Pampillo Baliño.

Quiero reflexionar sobre este tema tan extraordinariamente complejo, novedoso y que es un tema que a mí me llena de perplejidades antes que de certezas, que es precisamente el de los desarrollos normativos en el contexto de la globalización.

Quiero también aclarar que a pesar de que se me ha presentado como abogado de IBM, no vengo aquí, en esta tarde, en calidad de abogado de IBM, sino en calidad de abogado o de profesional del Derecho a título estrictamente particular y, en todo caso, en mi condición de

[2] Privación de datos, aviso, limitación a la recolección, uso de información personal, salvaguardas de la seguridad, acceso, corrección y responsabilidad.

académico y de profesor de Derecho en otras universidades.

De manera tal que la posición, las perspectivas y los conceptos que quisiera yo compartir con ustedes y someter, desde luego, a su consideración, son conceptos, perspectivas y ángulos estrictamente personales, que en modo alguno responden a la posición oficial de la empresa para la que laboro.

En tercer lugar, quisiera también resaltar como cuestión de previo y de especial pronunciamiento, como dicen los abogados procesalistas, que ante el inmenso reto de presentar y de someter a la consideración de ustedes una ponencia sobre este tema tan rimbombante, pero a su vez tan profundo y tan radical *Desarrollos Normativos en el Contexto de la Globalización*, realmente no supe encontrar la forma de aterrizarla a manera de ponencia, porque, como les intimaba hace un instante, realmente es un tema éste que ha creado en mi ánimo y que me permite decantar también en mi pensamiento, un cúmulo de dudas, un cúmulo de preguntas, un cúmulo de interrogantes, que no de certidumbres, que no me permiten propiamente que le imprima, por así decirlo, a esta exposición, el cariz de una ponencia, sino más bien de un cuestionamiento.

Es un cuestionamiento, a su vez, que recoge en parte los planteamientos de quienes me han precedido en el uso de la palabra.

Quiero citar, por ejemplo, al doctor Travieso, que nos decía hace unos instantes, precisamente en su Conferencia Magistral, cómo nuestro tiempo es un tiempo de la tecnología; esto es, de la razón de la técnica, pero también del tecnonihilismo.

Nos decía también y nos hablaba de cómo vivimos en tiempo real y sin embargo parece que no tenemos tiempo para nada. Y nos hablaba de una cuestión que es igualmente fundamental, de cómo nuestra época, la época de la globalización, es una época de cambio de paradigmas.

Igualmente, mi colega el profesor David Banisar nos hablaba precisamente de los contrastes en los entrecruzamientos que se producen precisamente entre el Derecho, o más bien, el tema de la protección de los datos personales, vistos desde el ángulo de Derecho fundamental, pero visto también desde el contrapunto, precisamente, de los derechos comerciales. Contrastes, contrastes que crean dudas y perplejidades y no certezas ni convicciones.

Y también Jesús Orta nos hablaba hace unos instantes de la sensibilidad, que la sensibilidad propia y característica de la sociedad de nuestro tiempo, de la sociedad que nos es contemporánea, nos ha impuesto respecto de este tema, que no era tan importante hace apenas unos 50 años.

Y reflexionando sobre estas perspectivas de los colegas que me antecedieron en el uso de la palabra, refrendo mi perplejidad respecto de este tema, por tres razones fundamentales: En primer lugar porque se trata propiamente del tema de la protección de los datos personales, de un tema que yo caracterizaría como un tema límite o frontera.

Un tema límite o frontera que se encuentra en algún lugar que está por ahí en medio del ámbito de lo privado, pero también, por así decirlo, de la comarca de lo público, donde se produce, como en todo lugar de encuentro, una especie como de choque entre intereses entrecruzados

Y específicamente por lo que respecta a mi disciplina, por lo que hace a la ciencia del Derecho, se encuentra este tema apasionante de la protección de los datos personales, a caballo precisamente entre los distintos ámbitos de la ciencia del Derecho Constitucional, de la Ciencia del Derecho Civil, de la Ciencia del Derecho Laboral.

Se trata, pues, en definitiva, el tema central de la protección de los datos personales, de la protección de la privacidad de los datos personales, precisamente en este lugar de encuentro.

Pero además de ser un tema límite, es un tema transfronterizo, precisamente porque los problemas sociales, que supone precisamente la protección de la privacidad de los datos personales, son problemas que exceden y rebasan toda localización y, por ende, la problemática social que plantean no es una problemática social susceptible de ser reconducida desde una perspectiva localista ni regionalista, sino precisamente global, máxime consideren ustedes como el tema precisamente de los derechos de la intimidad cuando sufre una revolución que lo exponencia precisamente creando esta mayor sensibilidad en nuestro tiempo, ante los peligros que supone el manejo inescrupuloso de sus datos personales, se ve precisamente potenciado con motivo de la revolución tecnológica y muy acusadamente a partir de la década de los ochenta.

Porque, precisamente dada la irrupción del fenómeno de la globalización informática, fenómeno éste que supone que en algún lugar, casi por recordar la obra de Tomás Moro, utópico esto es, en ningún lugar, utopo significa en ninguna parte, pero utópico que no se encuentra localizado en ninguna parte pero que a su vez se encuentra en todos los lados, ubicuo, ucrónico porque no es que lo que suceda en la red acontezca en algún tiempo específico, sino que acontece de manera simultánea en todo tiempo.

De manera tal que por su misma deslocalización geográfica de un lado y, cronológica de otro, el fenómeno de la red de redes supone el fenómeno de problemas que son actuales, contemporáneos, sincrónicos y que se producen de manera simultánea en todo tiempo y en todo lugar. De ahí la dimensión exponencial y gravísima del tema de la protección de los datos personales.

Y en tercer lugar digo yo que es un tema complejo, precisamente en virtud de que es un tema que pertenece a una época muy propia de nuestro tiempo, a una época que ciertamente no parece ser ya más la época contemporánea, sino una época en la que claramente, recogiendo de nueva cuenta la expresión afortunada del doctor Travieso, es una época en la que nos encontramos ante la existencia de nuevos paradigmas.

Pero yo diría más, no solamente de nuevos paradigmas, nos enfrentamos también a la realidad de que los paradigmas fundacionales de nuestra cultura y de nuestra civilización, son paradigmas que se encuentran en crisis y al lado de estos paradigmas que se encuentran en crisis, surgen y aparecen otros nuevos paradigmas emergentes que se debaten respecto de estos otros paradigmas en crisis anteriores, precisamente la prevalencia fundacional, por así decirlo, de las actitudes propias y características del hombre inserto dentro de una determinada civilización y dentro de una cultura específica.

Voy a tratar a partir de estas tres perplejidades fundamentales que me suscita este tema, de proponerles a ustedes, porque les insisto, yo no vengo a manera de ponente a plantearles otras cosas, sino precisamente cuestiones que a mí me ha suscitado la reflexión de este tema y que son cuestiones muy puntuales.

Respecto del primer punto hay que entender, y yo creo que es muy importante que tengamos ese punto de partida, que el tema de la protección de la privacidad de los datos personales, es un tema que se caracteriza por su interdisciplinariedad y consecuentemente es un tema que no puede abordarse, sino precisamente desde una relativa contaminación metodológica, donde no cabe purismos ni cabe tampoco la asepsia, sino que es menester que nos enfrentemos a una realidad, por así decirlo, que tal y como se nos aparece, tal y como se nos plantea. Se nos plantea contaminada precisamente a partir de su pertenencia a muy distintos ámbitos sociológicos de un lado y jurídicos de otro.

En segundo lugar, precisamente por virtud de esta ubicuidad global de los fenómenos informáticos, es necesario que partamos de la premisa fundamental, a mi modo de ver las cosas, de que tratándose como se tratan los problemas que nos ofrece precisamente el flujo, la

recolección y la circulación de estos datos personales, como se trata pues de un fenómeno eminentemente global son necesarias soluciones igualmente globalizadas y de esta forma no pueden considerarse sino como principios de solución, como puntos de partida hacia una solución definitiva y eficaz de estos problemas suscitados por la protección a la privacidad de los datos personales, aquellas soluciones locales y regionales.

Es menester que se busquen nuevas y novedosas fórmulas de armonización jurídica que permitan reconducir precisamente de manera eficaz y comprensiva estos problemas sociales; y en tercer lugar, respecto de cómo estos problemas suscitados por la protección de la privacidad de los datos personales son problemas propios de nuestra época, y cómo responden precisamente a una sensibilidad mayor de nuestro tiempo. Por lo que respecta precisamente a la proyección de los derechos propios de la intimidad, es necesario también que reflexionemos cuáles debieran ser los valores conforme a los cuales dichos problemas debieran abordarse en el contexto de la globalización.

Partiendo de estas premisas, por así decirlo, ordenadoras, y que más que premisas ordenadoras suponen ante todo unos referentes que nos permiten dimensionar la complejidad y hasta cierto punto la inaprensibilidad de los problemas propios de la protección de los datos personales, las preguntas o los planteamientos que yo quisiera dejar como parte de esta exposición son fundamentalmente los siguientes:

En primer lugar, ¿es posible la regulación de la protección de la privacidad de los datos personales a través de las legislaciones de los Estados nación?, ¿es posible?, ¿es realmente posible? En segundo lugar, en caso de no serlo o de serlo sólo relativamente, ¿pueden considerarse como alternativas razonablemente sustitutivas de la legislación de los Estados los distintos acuerdos regionales o universales, en todo caso multilaterales celebrados por distintos Estados, con el propósito de armonizar y relativamente homologar los criterios para la protección de los datos personales?

Una tercera pregunta más radical que presupone precisamente las dos interrogantes anteriores, ¿es posible a la postre elaborar un desarrollo normativo de cualesquiera índole para efectos de regular la debida protección de los datos personales? Y en todo caso este tipo de regulación, ¿qué tipo de regulación debiera ser? ¿Debe ser una regulación autoimpuesta, autorregulada, realizada por la industria o debe ser una heterorregulación? En todo caso si se trata de una heterorregulación, ¿cuáles serían los centros de creación jurídica de estas soluciones para reconducir este problema: el Estado, las regiones, las empresas, la industria, etcétera? Y, ¿qué tipo de normatividad jurídica sería necesaria para reconducir este tipo de problemática, una ley en el sentido de *Harlock* como se denomina actualmente en el ámbito de las comunidades europeas o de *Softlock* como parecieran indicar ciertas recomendaciones dadas en el seno de las comunidades europeas?

En fin, son muchos los temas de los que pudiéramos hablar respecto de los desarrollos normativos en el contexto de la globalización. Yo me permito limitarme únicamente a suscitar estas inquietudes que me ha provocado la reflexión respecto del tema, y prefiero, si así están ustedes de acuerdo conmigo, en que abramos el espacio, si acoso el tiempo lo permite para preguntas y respuestas, y seguir dialogando sobre este tema.

Moderador: Isidro Cisneros. Profesor Investigador de la Facultad Latinoamericana de Ciencias Sociales –FLACSO– México.

Le toca el turno a Roberto Andrade Martínez, es licenciado en Derecho, egresado de la Universidad Latinoamericana, postgrado en Derecho Mercantil por la Universidad de Salamanca, España, y actualmente forma parte de la Junta Asesora de Latinoamérica Law Institute de la Universidad de Tulane. Ha sido abogado de Martínez, Algaba, Estrella, De Haro, Galván, Duque. Gerente Jurídico de Exon Móvil

México, Director Jurídico de Panasonic México, y actualmente es Subdirector Jurídico de Telefónica Móviles-México.

Ponente: Roberto Andrade Martínez.

Mi idea aquí es un poco transmitirles qué es lo que estamos haciendo desde el Grupo Telefónica Móviles-México respecto a este tema de protección de datos.

La empresa se encuentra no preocupada, pero sí muy interesada, y toma esto muy en serio.

Nosotros actualmente enfrentamos diversos problemas al tratar de emitir un código tipo dentro de cada uno de los países debido a las diversas legislaciones o la falta de legislaciones en algunos casos.

Voy a tratar aquí tres temas, que es la protección de datos de Grupo Telefónica, cual es el presente, futuro, y los próximos pasos que pensamos dar.

El siguiente sería la implantación de códigos tipo de todas las empresas de Telefónica, estaríamos implantando tomando como el modelo de Telefónica España.

La tercera fase es el diseño de unas normas corporativas vinculante, Binding Corporate Rule, en las cuales tenemos la intención de que todos los países podamos homogenizar la protección de datos en una empresa de telecomunicaciones que todos los días va innovando y va obteniendo nuevos retos.

La situación actual, parte difícil, la inexistencia de una política corporativa de protección de datos, no tenemos una política global donde todos los países de alguna manera hayamos homogenizado el tratamiento de protección, el tratamiento de datos.

En la mayoría de los países donde nosotros nos encontramos o tenemos presencia hay una ausencia de regulación.

¿Cuáles son las previsiones futuras? Lo primero es diseño de una política corporativa de protección de datos.

La compatibilidad de las distintas regulaciones, se imaginarán ustedes el problema que es hablar con cada uno de los países y tratarles de explicar que tenemos todos que ponernos de acuerdo cuando tres o cuatro personas nunca nos ponemos de acuerdo en un mismo país.

La aplicación de principios y procedimientos comunes.

¿Cuáles son las ventajas que nosotros le estamos viendo a esto? Es la agilización de tratamientos de datos personales entre las empresas del grupo, importantísimo en nuestro negocio.

Obtención de la confianza en las autoridades regulatorias. Y una valoración positiva de los clientes, lo más importante.

Los próximos pasos los tenemos en dos fases: la primera, lo que les había platicado, la implantación de códigos tipo en todas las empresas del Grupo Telefónica. Y el segundo, es el diseño de las normas corporativas vinculantes.

Para lo que es la implantación de códigos tipo en las empresas de Telefónica, es el establecimiento de un marco de obligado cumplimiento en el grupo que garantice un nivel mínimo de seguridad en el tratamiento de los datos de carácter personal.

En concreto, las obligaciones de la empresa y el deber de confidencialidad, una de las partes más importantes es la confidencialidad y las obligaciones que la empresa tiene que tomar para la protección de los datos que tiene en su poder o que se ha hecho de su poder por diferentes situaciones.

El tratamiento de los datos de carácter personal y la transferencia internacional de los datos, punto importantísimo para nosotros.

Diseño de procedimientos comunes de actuación en materia de protección de datos.

Lo primero que tenemos que hacer en una empresa cuando esta materia es nueva es la identificación de los ficheros de carácter personal; uno tiene que ir con cada una de las áreas y decirles: ¡Oye!, aunque tú no lo sepas tienes esta información muy importante que pertenece a cada uno de los individuos a la cual tú se lo solicitaste en algún momento.

Ustedes se sorprenderán que digan:
-No es cierto, nosotros no tenemos eso.
-Les digo, ¿cómo no?
-Pero es que nada más tengo el nombre, la dirección, el teléfono; si es casado, si es soltero.
-Tiene una cantidad de información.

Entonces, lo primero que tenemos que hacer es ir con las áreas y con cada una de las áreas lo que tenemos que decirles es: ¡Mira!, toda esta información pertenece a cada uno de los señores que te la proporcionó y lo que tenemos que darle es un debido cuidado.

Lo primero, por consecuencia, es sensibilizar a las diferentes áreas de los diferentes países; imagínense esto hacerlo a nivel global.

El control de los ficheros es la misma situación. Tenemos que organizarnos de alguna manera ya que si estamos nosotros en 19 países del mundo, hablar con ellos y decir, vamos a tener un control porque va a haber o queremos tener un intercambio de información.

Para lo cual tenemos que garantizar la seguridad de datos. Vamos a ver cómo tienes organizado y cómo tienes controlados tus ficheros.

Tratamiento y uso de datos personales, los principios. Lo primero que tenemos es tener una recopilación lícita y leal de los datos, respetando la obligación de información y consentimiento de los afectados.

La veracidad de los datos. Los datos deberán ser exactos, puestos al día en forma que respondan con veracidad la situación actual del afectado, es importante que sean exactos y que se encuentren actualizados.

La conservación limitada de los datos en función de su destino, serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad a la cual hubieren sido recabados o registrados.

Cuando uno recaba datos tiene una finalidad, tendrá un proyecto. Este proyecto o la razón por la cual se obtuvieron esos datos tiene una caducidad, yo no soy un banco de datos para estarme haciendo de ficheros en los cuales después yo no les puedo dar un debido mantenimiento, porque al final de cuentas a mí ya no me interesa.

Seguridad física y lógica de los datos. Garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Los niveles de acceso a los datos. Los datos se encuentran en la empresa a disposición de los empleados y de diferentes personas dentro de la misma empresa, pero con grados de acceso; no todas las personas podrán acceder, digamos, al *fail* que se tiene o al fichero que se tiene, de recursos humanos, donde vienen los datos sobre la persona, sobre su sueldo y demás. Tendrán que estar limitados sobre grados de acceso y limitantes en éste.

Tenemos la implantación de códigos tipo de las empresas. Otros temas de consideración contienen el código tipo de Telefónica España, que es el que estamos tratando de utilizar como un marco de referencia, es el acceso de los empleados a la información de los clientes, lo que les acabo de comentar, el movimiento internacional de datos y la adaptación de medidas de seguridad.

Y este es nuestro verdadero reto: Llegar a un diseño de Normas Corporativas Vinculantes o *Binding Corporate Rules*, que son instrumentos potenciados por la Unión Europea, enfocado a

flexibilizar los movimientos internacionales de datos. Las ventajas nos facilitan las transferencias internacionales intragroup, mejora el cumplimiento de la normatividad de protección de datos.

¿Qué desventaja le estamos viendo nosotros?

Sólo son aplicables a las transferencias internacionales entre compañías del grupo y pueden configurarse como mínimos si la legislación local es más exigente.

Para nosotros poder facilitar, para que la empresa, para que la corporación pudiese realizar de manera continua, fácil y ágil, las transferencias internacionales de datos, que es una de las partes de la globalización, necesitamos nosotros tener implementadas estas Normas Corporativas Vinculantes, donde en algunos países, en los cuales nosotros tenemos presencia, no existe una legislación que le dé una seguridad a la Unión Europea, en este caso, sobre el tratamiento que se le va dar a los datos que se estarían transmitiendo.

Entonces, ¿qué es lo que nosotros tenemos que hacer? Pues adecuarnos al organismo regulador y decirle: Ya estamos listos, tenemos nuestras normas corporativas vinculantes e independientemente que en todos los países estaban trabajando los diferentes gobiernos para regular este tema, nosotros ya estamos listos, como compañía.

Fases y el diseño de implantación. El período que nosotros nos estamos poniendo es del 2005 al 2008. Parecería un poco largo, pero en realidad no lo es. Estamos en la constitución de grupos de trabajo en el país, que al día de hoy ya los tenemos; un análisis marco normativo por país.

Ha sido algo difícil en algunos países, porque han tenido que hacer una recopilación de diversas aplicaciones o de diversas legislaciones, donde habla un poco o casi nada o quieren hacer referencia o quieren relacionarlo, cuando en realidad no lo es, a la protección de datos.

La elaboración y remisión de los primeros análisis a las secretarías generales del país, donde nosotros al día de hoy, en este momento nos encontramos. Tenemos que diseñar un plan de implantación, elaborar y remitir un informe de las valoraciones que se hicieron en cada uno de los países y la implantación.
Como ven, para Telefónica este es un tema importantísimo y en todos los países estamos trabajando arduamente.

Nos hemos planteado una fecha, una fecha que para nosotros es un reto importante, pero sé que los vamos a lograr.

Moderador: Isidro Cisneros. Profesor Investigador de la Facultad Latinoamericana de Ciencias Sociales –FLACSO– México.

Tendremos unos minutos que quisiera que aprovecháramos de la mejor manera para preguntas del auditorio a nuestros conferencistas.

Pregunta: Alonso Lujambio, Comisionado del IFAI.

Me han parecido especialmente interesantes las reflexiones que haz hecho, Jesús. Si lo vemos desde una perspectiva estrictamente doméstica, necesitamos un equilibrio, sí, entre privacidad y flujo de información comercial, esa es la posición que ha asumido el IFAI.

Desde una perspectiva internacional, tenemos compromisos con la Unión Europea, estamos en la APEC, estamos en el entorno del Tratado de Libre Comercio con nuestros socios comerciales y tenemos ahí demandas, ciertamente o compromisos aparentemente contradictorios.

Hablas de un equilibrio, que se busca la convergencia, nunca desarrollaste, en qué consiste el equilibrio desde la perspectiva tuya o de la Secretaría de Comercio. Creo que ahí está una clave de nuestro debate y me gustaría que desarrollaras un poco, por lo menos por dónde se van perfilando esos equilibrios.

Otra cosa que te pregunto. Dices, *no hay conciencia*, te cito, *no hay conciencia generalizada sobre la cuestión de la privacidad en América Latina*.

Yo te pregunto si eso lo juzgas positivo, como un hecho neutral o si lo juzgas negativo. Porque entiendo que la conciencia es un valor positivo y que tú digas que no hay conciencia generalizada, supongo que estás haciendo un juicio valorativo sobre esa realidad.

Juan Pablo, hablas de tres perplejidades, pero voy a mencionar una cuarta que es la que me produce tu ponencia. Me sorprende que alguien que expresa de manera tan elocuente tanto talento, no asuma una posición, aquí vinimos a asumir posiciones.

Quiero que me respondas una pregunta clave y sé que la puedes responder, pero de ahí se derivan muchas consecuencias: datos personales. Ese es un concepto que tú avalas, porque lo usas.

Yo te pregunto: ¿Quién es propietario de los datos personales que tiene una empresa, la persona o la empresa?

Creo que cualquier respuesta que des a esa pregunta se deriva una serie impresionante de consecuencias y me gustaría que un poco especularas sobre ella, aprovechando el talento que tienes y que no te nos vayas sin que lo exprimamos.

Pregunta: La presente pregunta va dirigida a Juan Pablo Pampillo.

Respecto a la explicación que nos ha hecho ver a lo largo de este espacio, quisiéramos saber si la postura sobre la cual versó esta explicación es personal o bien si nos está hablando a nombre de la empresa de IBM.

Si es personal, ¿cuál sería entonces la postura que está asumiendo IBM respecto del tema que nos ocupa?

Pregunta: José Luis Piñar.

Yo creo que la mesa ha sido enormemente interesante, pero yo creo que en efecto y coincido con alguna otra pregunta, falta o hecho de menos alguna posición más concreta y definida.

Se ha puesto de manifiesto una tensión en los planteamientos que han estado sobre la mesa, que es la tensión entre marco o modelo de regulación, modelo de autorregulación.

Creo que la última ponencia de Telefónica ha sido muy equilibrada, sin embargo en este punto al distinguir perfectamente entre los modelos de regulación y lo que se debe hacer desde una empresa multinacional para intentar garantizar que en todos los países, incluso donde no hay una legislación de protección de datos se respeten los datos personales.

Pero mi duda es, lo planteo a la mesa en general y a ninguno en particular. Vamos a ver, si estamos hablando de un derecho fundamental, yo creo que todos estamos de acuerdo en que estamos hablando de un derecho fundamental, como es el derecho a la protección de datos personales, cómo es posible dejarlo de la mano sólo de la autorregulación o señalar que hay dos modelos: el de autorregulación o el modelo normativo.

En los textos internacionales como la Declaración Universal, Derechos Humanos, pactos, derechos libres y políticos, Convenio 108, Carta Europea, Pacto de San José de Costa Rica, no recuerdo ni un solo caso en que se haya dejado la regulación de un derecho fundamental al modelo autoregulatorio, ninguno.

En todos, en ningún caso se dice que quedará en manos de los actores el regular el contenido de un derecho fundamental, siempre se exige que los Estados adopten textos normativos que garanticen el derecho fundamental.

Entonces mi pregunta es: ¿No estaremos aquí planteando no un debate entre autorregulación

y regulación o marco normativo sino entre intereses contrapuestos? ¿No estaremos aquí hablando realmente de determinados intereses que prefieren un marco de autorregulación antes que la imposición de un marco regulatorio? Si aquí se ha dicho incluso que estamos por encima de marcos normativos nacionales dado el carácter transnacional de la protección de datos, cómo es posible que se opte como modelo, no de convivencia, sino modelos alternativos, que ese es el problema, el problema no es plantear que convivan dos modelos, sino modelos alternativos, ¿cómo es posible que se plantee como modelo alternativo el que las propias empresas sean las que regulen el contenido de un derecho fundamental, como es la protección de datos?

Pregunta: Es para a Jesús Orta, ya que él es experto en la APEC. Hace poco en la revista *Etcétera* apareció el caso de un periodista chino que hizo una denuncia en una de estas comunidades de Internet, y la empresa Yahoo, que proveía el servicio dio la información de quién era este periodista y fue arrestado por las autoridades de ese país, tengo entendido que Yahoo hizo un convenio precisamente con las autoridades chinas de respetar las leyes chinas, y entre ellas se encuentra precisamente el de hablar en contra de las autoridades.

Yo quisiera una aclaración a este tipo de cosas, porque si estaba hablando de la normatividad internacional acerca del respeto, en este caso a la protección de datos personales, ¿cómo es que se da un ejemplo tan flagrante de violación a los mismos?

La pregunta es para el doctor David respecto a la diferencia que él establece entre la visión estadounidense y el de la Comunidad Europea respecto a la protección de datos personales, si tiene que ver en algún sentido; me extraña, porque el origen del derecho norteamericano obviamente es el derecho inglés, pero no sé si en la Comunidad Europea es por la relación que hay de dos tradiciones jurídicas distintas. Una que es la del Common Law, y la otra es la del Derecho Romano, bueno, el Derecho Civil de origen neorromanista, si tiene que ver algo este aspecto.

Y finalmente quisiera preguntarle a la persona de Telefónica si considera que esta normatividad que ellos están dando va a incidir, en este caso, en México, porque entre los planes de Telefónica, tengo entendido, está próximamente entrar en competencia con Telmex que es uno de los grandes violadores precisamente de datos personales de este país.

Me gustaría saber, si eso va a promover una competencia que van a ser más competitivas las empresas que ofrezcan precisamente una mejor protección a datos personales. En este caso si es Telefónica en comparación con Telmex.

Pregunta: Les agradecería si me dieran la oportunidad de llevarme algo concreto de esta reunión. Escuché al maestro Juan Antonio Travieso, y lo he escuchado en otras ocasiones de que la única ley que se cumple en Latinoamérica es la de la gravedad.

Después de escuchar todas las disertaciones que me han parecido bastante interesantes, análisis profundos, detallados, en lo que es la problemática de la protección de los datos personales, pero en un entorno como el que menciona el maestro Travieso y otro panelistas latinoamericanos pues realmente me lleva a un río bastante fuerte, en cuanto lo que sería la estrategia de venta para aquellos que hacen posible que se vuelvo algo concreto, específicamente a lo que son nuestros gobiernos.

Yo le a agradecería los panelistas si pudieran darme al menos un acercamiento, una aproximación de lo que sería una estrategia de venta e implementación del resultado de sus disertaciones y análisis en Latinoamérica sobre la protección de datos personales.

Pregunta: Octavio García Ramírez, el de la voz. Inicialmente felicitar a todos y cada uno de los ponentes por parte del Consejo Nacional de Jóvenes; preguntarle a nuestro amigo representante de la República Argentina, ¿cuál

fue su experiencia acumulada particularmente en materia del ámbito financiero? Al igual que al amigo representante del Reino Unido.

La pregunta se enfoca al ámbito financiero en su país, sobre ¿cuál ha sido la experiencia en ambas naciones?

Ponente: Roberto Andrade.

Primero trataré de contestar la pregunta o una de las preguntas que hizo José Luis Piñar.

Aquí la situación es difícil, nosotros somos una empresa y nosotros tenemos que trabajar en un mercado, tenemos una tecnología que va avanzando, estamos posicionados en diferentes países y nosotros no nos podemos esperar a que los gobiernos decidan.

Me encantaría que en todos los países donde nosotros tenemos presencia existiera una verdadera regulación sobre protección de datos, pero no es la realidad.

Y yo como empresa no me puedo esperar o no me puedo dar el lujo de que los gobiernos en que en algunas ocasiones actúan eficientemente y en otras no regulen, y entonces sí nosotros arranquemos, yo creo que eso para una empresa transnacional y una empresa de vanguardia es imposible.

Entonces, como Telefónica no nos daremos ese lujo y si el gobierno nos pide nuestra ayuda, siempre contará con ella, estaremos coadyuvando para que en ningún momento se diga que los particulares no quisieron participar o le temen a tomar una postura respecto a la protección de datos. Esa es la primera.

En la segunda, ya estamos en el mercado, estamos luchando tú a tú con Telmex, pero nosotros con una propuesta diferente, nosotros tenemos una propuesta de innovación y tenemos una propuesta ética y dentro de esa propuesta ética viene la protección de los datos de nuestros clientes.

Cuente usted que si se convierte en cliente de Telefónica sus datos estarán protegidos.

Ponente: Jesús Orta Martínez.

Primero, Comisionado, la razón por la que yo no pude hacer una exposición más amplia sobre qué significa para nosotros el equilibrio, es porque me dieron 10 minutos y ciertamente es muy difícil.

Déjame decir rápidamente qué quiere decir equilibrio y lo voy a tratar de decir con un ejemplo para ser concreto y breve. Con todo respeto obviamente a los distintos enfoques normativos que existen en diversos países en el mundo.

En materia de flujos transfronterizos de datos. Para nosotros no es una postura que favorezca el equilibrio el exigir a un Estado un grado de protección a nivel legislación como condición para poder transferir datos, eso es una cuestión que atenta contra el equilibrio en cuanto al flujo de los datos.

¿Qué sería algo que sí lo favoreciera? Voy a establecer las salvaguardas necesarias y eso puede ser a nivel de relación contractual entre privados y de ahí déjenme aprovechar para contestar una segunda inquietud; de ninguna manera el gobierno mexicano está proponiendo el que no haya una regulación sobre un derecho fundamental, de ninguna manera. En México va a haber ley sobre la materia. Ahorita se está discutiendo, tiene cinco años en discusión, pero va a haber ley, de eso no debe haber duda.

Lo que estamos diciendo es que a favor de ese equilibrio debe haber, si tenemos que respetar y eso es lo que tenemos que hacer, la tradición jurídica o el enfoque normativo que tome un país, eso no puede por sí mismo limitar los flujos de datos.

Tienes que encontrar alternativas y entonces la alternativa puede ser, desde nuestro punto de vista, que las relaciones contractuales entre privados puedan hacer las veces de factor de equilibrio.

Es decir, al mismo tiempo que a nivel nacional provees legislación para proteger los derechos, en este caso de la protección de datos o la privacidad de los individuos, también favoreces el flujo de datos.

Y aquí no hay que perder de vista que estamos hablando no solamente de un derecho fundamental consagrado en diversos documentos, sino también estás hablando de la viabilidad de un modelo económico que nos es inevitable a todos, que es: Cadenas de valor globales. El ejemplo de Telefónica es muy claro. Para poder operar en diversos países si Telefónica va ha mandar datos sobre su nómina a su corporativo en España o en donde lo tenga, pero la legislación impide que así sea por cuestiones de privacidad, donde evidentemente no va a haber, tratándose de arreglos corporativos éticos, sólidos, no puedes limitar el flujo de estos datos, tiene que haber alternativas. Y allí es donde hablamos de un equilibrio.

De ninguna manera estamos, como gobierno, tratando de reemplazar la regulación formal, es decir, la ley o cualquier ordenamiento jurídico o lo que sea, sino tratando de establecer lo necesario, con complementos, para poder garantizar ese equilibrio.

Sobre el juicio, sobre la sensibilidad, es malo que no haya conciencia, por supuesto. Si se interpreto que yo decía que era bueno, pido una disculpa; no, de ninguna manera.

Lo que quiero decir es que es un hecho que no hay una alta sensibilidad en la región y en otras, hacia este tema. Me refiero a una sensibilidad generalizada. Sí la hay, por supuesto, en capas específicas de la sociedad.

Casos como el de China se mencionaban. Por supuesto que aun y cuando haya leyes y demás, siempre va a haber violaciones a la privacidad.

Y alguien hablaba sobre proponer una estrategia en Latinoamérica o algo así. Yo diría que es muy difícil. Es muy difícil, porque sólo por mencionar rápidamente el ejemplo de México, la situación de México es muy distinta a la de cualquier otro país latinoamericano y nada más voy a dar un dato del por qué.

El volumen de comercio entre México y Estados Unidos es mayor que el del resto del comercio intralatinoamérica, es decir, entre todos los países de Latinoamérica.

Entonces, si tenemos en cuenta eso es obvio que para el MERCOSUR es un contexto distinto que para México en sus relaciones, hablando en lo comercial, ya no digamos sobre otros aspectos que naturalmente también hay cuestiones de divergencia potencial.

Ponente: Juan Antonio Travieso.

Veo que ha generado muchas dudas e inquietudes y muchas veces el tiempo es un verdadero elemento que nos obliga a hacer esta posdata, el *Post Christum*, que muchas veces es tan importante. Y por eso, entonces, vamos a hacer los Post Christum.

A la pregunta de José Luis, a la participación de José Luis, le quiero decir que quizá como se omitió mi presentación, quizá no se aclaró que yo soy profesor de Derechos Humanos y yo considero y tengo escrito en muchos libros el tema acerca de que los Derechos Humanos son básicos e incluso la cuestión de la protección de datos. Lo he escrito en el año 1981, en mi primer trabajo en un libro que fue galardonado con el premio de UNESCO.

Así que quizás en un tiempo en que posiblemente José Luis todavía no soñaba con desempeñar el cargo que está desempeñando, yo ya dije y sustentaba que era un derecho fundamental, sostenido desde el principio de la convención de 1981 que fue la señera y tal es así que en el próximo mes de marzo vamos a invitar a que asista a la Argentina, en los últimos días de marzo, vamos a tener la presencia del que primero habló de los derechos fundamentales de la protección de datos que es el señor Spiro Simités, así que muy buena la participación de José Luis en este sentido.

Solamente quiero agregar que cuando se habla de marcos autoregulatorios, por supuesto estamos hablando de marcos autoregulatorios en el seno de regulaciones jurídicas.

En la República Argentina en la Ley 25326 (Protección de los Datos Personales) se permiten códigos de conducta y ya tenemos aprobado un código de conducta en donde es un elemento muy dinámico poder producir un código de conducta que al mismo tiempo permita que la autoridad de control pueda ejercer su control sobre uno y sobre todos en forma rápida, eficiente y sencilla. Ese es el sistema a través del cual yo considero la autorregulación.

Sin duda hay regulación a través de los derechos fundamentales, hay regulación a través de los sistemas básicos que existen a nivel internacional, a nivel regional, etcétera.

Voy a la otra pregunta que es con respecto a la ley de gravedad. Y ahí por supuesto yo lo planteé como una hipérbole, discursiva, negativa. Es decir, lo planteé como un exceso en el cual yo dije hipérbole discursiva, negativa.

¿Qué quiere decir hipérbole? Es un término en el cual uno agranda una situación para que el espectador entienda una situación; al mismo tiempo es discursiva porque pertenece a un discurso.

Yo dije, no estoy de acuerdo con eso, tal es así que me emocionó cuando entregué los diplomas, los certificados de cumplimiento y la gente me dijo: gracias. Estabas cumpliendo con la ley, es decir, estoy seguro que eso habla de la tensión que ustedes han tenido. Y les agradezco muchísimo que me hayan considerado con tanta exactitud mis humildes palabras.

Y en tercer lugar, ¿cuál es la estrategia que podemos hacer?

Yo puedo hablar de lo que yo hago, la estrategia que tengo es múltiple, tengo muy pocos recursos, tengo la ayuda de los amigos, especialmente los amigos de España que son los que siempre me acompañan, no hay otros.

También cuando viajamos estamos difundiendo, esta es una estrategia de difusión con muy pocos recursos. Es decir, estamos explicando que esto se puede hacer, que no hacen falta grandes presupuestos.

Recién alguien me habló, no voy a decir quién, es un secreto de datos, alguien me dijo que en muchos casos, en determinadas estrategias se aplican enormes cantidades presupuestales y muchas veces el presupuesto es un obstáculo para poder hacer muchas cosas.

Debemos hacer un mentís a eso, el presupuesto no es un obstáculo, el obstáculo más importante es nuestra propia incapacidad, esa es la parte, el obstáculo más importante y nuestra propia ineficiencia, porque por supuesto tenemos ineficiencia, hacemos una autocrítica. Hay que difundir y en eso estamos.

Último muy rápido. Con respecto al sector financiero, por supuesto hay una estrategia muy grande que tiene que ver con una acción vinculada con la forma en que presentan los informes los bancos, en este caso nosotros estamos actuando dentro de los ciento y picos de bancos, en este momento ya se están inscribiendo en el registro de datos personales y al mismo tiempo actuar junto con el Banco Central para moderar la actividad del organismo central en materia de dictado de políticas monetarias.

Es decir, actuamos en forma concertada, protegemos a la gente, le posibilitamos el derecho de acceso, posibilitamos la supresión en un marco como es el argentino en el que se ha tomado una determinación de carácter estratégico financiero, que es la de no establecer el consentimiento para la información crediticia y para ella existe ese tipo de posición.

Es el área que más rápidamente ha aceptado el contralor, porque otra áreas son un poco más

renuentes, pero el área de los Burós de Crédito ha sido, no obstante los cuales para no monopolizar las respuestas me ofrezco para después darle con amplitud, incluso, estadísticas y presentaciones y todo lo demás a la persona que no puedo distinguir por la luz, pero que no dude al final de preguntar.

Ponente: David Banisar.

Voy a decirle algo sobre la Ley Inglesa contra la Ley Romana, entonces no hay una sola fuente en lo que es el derecho a la privacidad.

Tenemos muchos casos antiguos en Inglaterra, donde se han protegido a personas que, por ejemplo, cuando el rey les quitaba las casas, y casos en Francia durante el siglo XIX, cuando se violó el derecho a la privacidad. Hay muchas fuentes de sistemas legales distintos.

Y esto ha surgido como una combinación de muchos de ellos, y se ha desarrollado a partir de éstos. Hubo otra sobre la protección de datos financieros en el Reino Unido.

En general los registros financieros se protegen con una ley. Hay una ley general que protege todo tipo de datos personales y ha estado funcionando bastante bien. Hace poco hubo un caso en que el banco sacó algunos registros para una compañía hindú que estaba vendiendo los registros. Esto fue de hecho un robo de identidad, y como en cualquier otro sistema legal es más perfecto, pero creo que ha funcionado bastante bien.

Y finalmente el papel de las empresas. Se pensaba en 1995 cuando el Director de la Unión Europea veía la importancia de la privacidad por las corporaciones transnacionales, que querían trabajar mucho, y querían trabajar una sola norma y querían tener una sola directiva de privacidad, y no ha funcionado muy bien desafortunadamente.

También se han hecho esfuerzos más recientemente para cerrar la brecha entre lo que son las leyes de privacidad y la autorregulación y esto se ha desarrollado a través de las normas internaciones, a través de ISO.

Desafortunadamente estos se basaban en las normas canadienses. Son bastante buenas. Se desarrollaron en los bancos, en instituciones financieras, en algunos grupos que estaban trabajando juntos en Canadá, y la Organización Internacional de Estándares, y las organizaciones europeas tuvieron bastante sabotaje de las corporaciones estadounidenses y por eso no se llegaron a estándares generales.

Y fue una gran pena porque esto hubiera proporcionado muy buena información, y se hubiera difundido de una manera muy buena para no entrar en un modelo completo que sea autorregulatorio.

Ponente: Juan Pablo Pampillo Baliño.

Empiezo con la segunda pregunta, y empiezo por la segunda, porque yo creo que es segunda en tiempo, pero primer en términos de orden.

Como dije desde el principio de mi exposición, las perspectivas y ángulos que he querido externarles a ustedes son estrictamente personales, y desde luego no responsabilizo por ellas a IBM, en primer lugar.

En segundo lugar, cuál es la posición oficial de la empresa, pues desde luego de cumplimiento de la ley en todas aquellas jurisdicciones en las que ejerce el comercio, pero bajo la premisa fundamental, premisa ética fundamental de un estándar mínimo de eticidad en la conducción de sus negocios en aquellas jurisdicciones en las que no existe una legislación aplicable en materia de protección de los datos personales.

En este sentido yo diría que es una postura corporativa muy similar a la postura corporativa de Telefónica. Esto es de observancia del derecho, observancia estricta del derecho en aquellos países en los que existe un ordenamiento jurídico y regulatorio respecto del particular y en aquellas otras jurisdicciones en las que no existe un marco normativo en materia de datos

personales, tratar como estándar ético de ceñirse específicamente a los principios propios de la legislación norteamericana por virtud de la propia situación corporativa de la International Business Machines que se encuentra matrizada en los Estados Unidos de Norteamérica y obviamente los principios jurídicos norteamericanos permean toda su estructura.

Por lo que respecta a las preguntas del Comisionado Alonso Lujambio, en primer lugar, con toda sinceridad decir que si no he podido hacer otra cosa sino de exponer precisamente cuestiones e interrogantes que me ha suscitado la reflexión de este tema *desarrollos normativos y globalización*, es por aquello que decían los filósofos y los lógicos de que nadie da sino lo que tiene, y consecuentemente nadie da lo que no tiene.

Después de reflexionar respecto de este tema me quedan más dudas que certidumbres y he creído que la mejor forma en la que podía colaborar con esta mesa de trabajo era plantear precisamente estas dudas que a mí me suscitó la reflexión de este tema.

Por lo demás, por lo que respecta al tema de los datos personales sí decir que evidentemente yo creo que los datos personales son por así decirlo o el derechohabiente respecto de la protección de los mismos es precisamente la persona, y ¡ojo!, empleo precisamente el término persona en su acepción no solamente usual, sino específicamente etimológica y hasta filosófica, precisamente porque la persona no es el individuo, la persona es el individuo en su proyección social y consecuentemente la protección de la privacidad de los datos personales, si bien es cierto que le compete de manera directa e inmediata a la persona titular de los mismos, cierto es también que le interesa a la comunidad dentro de la cual dicha persona pues juega un determinado rol social.

Por último, por lo que hace al planteamiento de José Luis Piñar, yo me remitiría a la exposición inmejorable del doctor Travieso que a ese respecto recoge básicamente mis opiniones respecto del particular.

Protección de datos personales por los Gobiernos

Mesa 4:

Moderador: Alonso Gómez Robledo Verduzco: Comisionado del IFAI.

Carlos Arce Macías estudió la licenciatura de Derecho con Especialidad en Derecho Público en la Universidad de Guadalajara y en la Universidad de Guanajuato.

Se ha desarrollado como abogado del Consejo Nacional de Ciencia y Tecnología; maestro de la Facultad de Derecho de la Universidad de Guanajuato; oficial mayor de la Presidencia Municipal de Guanajuato; director ejecutivo de la Asociación de Municipios de México, A.C.; asesor jurídico del gobernador Vicente Fox, entre otros cargos.

Participó en diversos cursos y diplomados en Alemania, Costa Rica, Chile, Brasil, entre otros países. Se desempeñó como Coordinador Jurídico del Equipo de Transición del licenciado Vicente Fox Quesada.

Fue el titular de la Comisión Federal de Mejora Regulatoria, un órgano desconcentrado de la Secretaría Economía, de diciembre del 2000 a marzo del 2004; encargado del control de la normatividad del Gobierno Federal. Actualmente es Procurador Federal del Consumidor.

Conferencia Magistral: Carlos Arce Macías.

Agradezco la invitación a este IV Encuentro Iberoamericano de Protección de Datos Personales. Me da mucho gusto estar aquí discutiendo un tema tan importante para México.

Primeramente, sabiendo que en este encuentro participan, evidentemente, personalidades de otros países, con mucha puntualidad señalaré, en atención a ellos, el trabajo y la institución que represento, que es la Procuraduría Federal del Consumidor.

En la ponencia, primeramente, voy a hablar precisamente de qué es y qué hace PROFECO, la problemática en el manejo de datos personales y cerraría con una serie de soluciones que propondríamos, en relación a la Ley Federal de Protección al Consumidor, la óptica nacional, la óptica internacional respecto a PROFECO los consumidores y los datos personales, concluyendo evidentemente con las conclusiones a las que llego en mi presentación.

Primeramente qué es y qué hace PROFECO. Es un organismo descentralizado de servicio social, tiene personalidad y patrimonios propios, desarrolla funciones de autoridad administrativa.

Estas funciones son las relativas al encargo de proteger y promover los derechos de los consumidores, procurar la equidad y la seguridad jurídica en la relación entre proveedores y consumidores, y en ese sentido brindamos atención a los consumidores que no están de acuerdo con la relación que han establecido con los proveedores. Tramitamos anualmente cerca de 150 mil quejas de consumidores contra proveedores. En este sentido la PROFECO se convierte en un sistema de acceso a la justicia para un gran número de mexicanos.

También atendemos a los proveedores. Tenemos programas para mejorar precisamente todos sus sistemas de calidad y de atención al cliente.

Impulsamos el cumplimiento de la ley, en la cual tenemos una serie de funciones especiales, algunas de ellas, de las cuales voy a hablar, que tocan precisamente lo relativo a datos personales de una manera tangencial, y la parte probablemente más importante de PROFECO, que es la relativa a la educación del consumidor. A crear una cultura del consumo inteligente: Impulso al cumplimiento a la ley, educación a los consumidores, atención a los consumidores son los puntos vitales, los ejes principales del trabajo de la Procuraduría Federal del Consumidor.

Pasaré a la parte relativa a la problemática en el manejo de datos personales.

¿Cuál es la problemática que en estos momentos estamos enfrentando?

México no cuenta con un marco jurídico que regule el manejo adecuado de los datos personales. Ello evidentemente afecta al titular de datos personales, dado que su uso se hace de manera indiscriminada. Esto quiere decir, no sabemos dónde puedan acabar los datos personales de cada uno de nosotros. Pueden andar circulando hoy *ad limitum*, sin ningún tipo de regulación.

Para la política pública de protección al consumidor, las actuales prácticas de mercadotecnia directa e indirecta, en algunas ocasiones, no hacen un uso adecuado de los datos personales. Simplemente si nos vamos nada más a la parte de mercadotecnia tanto directa como indirecta, veremos que de repente llega una serie de publicidad que no sabemos cómo llegaron nuestros datos, nuestro domicilio o bien nuestro número telefónico a manos de ciertas empresas.

El titular de los datos, el consumidor, resulta afectado por prácticas comerciales que pueden ser engañosas e incluso fraudulentas tanto a nivel nacional como internacional.

Yo quiero comentarles que durante mi permanencia en la COFEMER, en la Comisión Federal de Mejora Regulatoria, ahí procesamos lo que fue, sobre todo la iniciativa de acceso a la información, de la Ley Federal de Transparencia y Acceso a la Información. Ahí la construimos, y la promovimos junto con algunas otras instancias de gobierno; pero precisamente durante este proceso de construcción de la Ley Federal de Transparencia y Acceso a la Información, y analizando sobre todo el derecho comparado nos quedo, desde entonces, muy claro que a México le faltaban otras dos leyes para complementar el paquete precisamente de transparencia y no era otra cosa sino dos leyes importantes: La Ley de Archivos y, por supuesto, la Ley de Protección de Datos Personales.

De tal manera que este paquete, que tiene tres pilares, hoy por hoy en México únicamente está sostenido en uno, que es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, pero le faltan estos otros dos instrumentos jurídicos tan importantes, como son la Ley de Archivos y la Ley de Protección de Datos Personales.

La problemática en el manejo de los datos personales. Esta institución, PROFECO, es especialmente sensible en el contexto de las tecnologías de la información y de la economía digital.

En México, en 2005 hay 17 millones de internautas, de los cuales casi el 73 por ciento son jóvenes y jóvenes adultos que van de los 13 a los 34 años. Estos grupos poblacionales son especialmente vulnerables a un mal manejo de sus datos personales en la transacción de bienes y servicios en línea.

Imagen ustedes que hoy por hoy gran parte del futuro del comercio es esencialmente el comercio electrónico y precisamente en la red van a estar subidos todos los datos personales o gran parte de nuestros datos personales.

¿Qué está pasando ahí? ¿Qué regulación hay en México? Es un gran reto, es un gran no solamente a nivel de México, sino realmente a nivel mundial.

Estos grupos poblacionales son especialmente vulnerables en estos servicios en línea y asimismo en el fenómeno de los correos electrónicos no solicitados o publicidad no solicitada en el Internet, como es el Spam. Tiene, entre otros orígenes, un manejo ilegal de bases de datos personales, además de que pueden ser vínculos para cometer prácticas fraudulentas.

Nuestro mail, nuestra dirección electrónica, ¿cómo llega a una enorme cantidad de empresas que luego nos mandan precisamente publicidad a nuestro correo electrónico?

Otra problemática, he hecho una lista de algunas cuestiones fraudulentas que hemos identificado desde la PROFECO, precisamente en el Internet, el llamado phishing, que no son otras cosas sino correos electrónicos falsos solicitando información financiera. Esto ha dado lugar a un sinnúmero de fraudes, sobre todo, correos electrónicos de bancos en los cuales solicitan números de tarjetas, números de cuentas, etcétera y luego vienen fraudes que pueden ser muy cuantiosos.

La carta nigeriana, acaban de pescar algunos nigerianos que hacían fraudes, se dedicaban a cometer fraudes aquí en México; sin embargo, esta carta no es otra cosa sino una solicitud de que le guarden dinero a un riquísimo rey nigeriano en el exilio que necesita poner su dinero en alguna cuenta, para eso le requieren a usted la cuenta y pues evidentemente va a tener grandes ganancias y con ese número de cuenta evidentemente viene el fraude; hay loterías y otros premios. Todo esto es esencialmente para captar datos personales de los cibernautas.

Servicios financieros que sea ofrecen, esquemas de trabajo en casas, ofertas, grandes ofertas de trabajos, empresas petroleras que ofrecen trabajos de tres meses en el Mar del Norte ganando miles de dólares al mes, en fin, venta de títulos y grados académicos, sin estudiar por supuesto, paquetes vacacionales, toda la parte de pornografía, adquisición de música y juegos.

¿Dónde están nuestros datos personales?, ¿cómo se protegen los datos personales?, ¿qué seguridad tenemos los consumidores en el momento de usar Internet? Cuando Internet se usa cada día más en la parte comercial.

Algunas soluciones. PROFECO, para empezar, visualiza una solución esencialmente global, ésta debe basarse en una combinación de marcos regulatorios claros, con prácticas éticas, que es lo que cerraría la pinza, las prácticas éticas por parte del sector privado.

Actualmente, el texto de la Ley Federal de Protección al Consumidor incluye elementos orientados a lograr una mejor protección de los datos personales en los consumidores, hay que recordar que la Ley Federal de Protección al Consumidor apenas acaba de sufrir modificaciones al respecto, acaba de expresarse estas modificaciones apenas en el 2004, empezaron a entrar en vigor en 2005.

Tenemos la función de poder ya establecer una lista telefónica para evitar las llamadas de mercadotecnia directa a las casas, en estas listas llamadas *No Call*, por ejemplo, de no llamadas, como hay en Estados Unidos y en otros países. Este es uno de los proyectos que esperamos avanzar de manera significativa en el próximo año desde la Procuraduría General del Consumidor.

Tenemos algunos datos importantes, algunas funciones en relación a mejorar la protección de datos personales de los consumidores.

Los elementos más destacados, el titular de los datos tiene derecho a saber si los proveedores poseen datos personales sobre él. El titular de los datos personales tiene también el derecho a acceder a sus datos y corregirlos, de existir errores o inconsistencias.

Los proveedores que poseen datos personales de los consumidores no pueden compartirlos o cederlos a terceras personas de manera indiscriminada.

Este problema, por ejemplo, ya lo vivimos en el caso de la base de datos de Direct-TV a SKY, precisamente en el momento en que se retira del mercado mexicano Direct-TV y queda nada más la empresa SKY como la oferente de los servicios de televisión satelital.

Los proveedores no podrán usar esta información con fines distintos a los originales, o sea, exactamente los establecidos en su negocio, no pueden, en principio, estar pasando las bases de datos indiscriminadamente a otros comercios, a otras corporaciones.

Y desde la óptica nacional se debe reconocer cabalmente la inserción de México en la globalización y en las innovaciones tecnológicas, hay que aceptar el nuevo ambiente económico general y para los actos de consumo en particular, por ello la PROFECO busca fortalecer la protección y defensa de los derechos de los consumidores en un nuevo contexto digital.

PROFECO busca crear mayor conciencia entre los consumidores de lo que puede implicar el mal manejo de sus datos personales, sobre todo en el contexto electrónico.

La visión, la perspectiva hacia futuro de la cuestión electrónica realmente no reconoce fronteras, ni ve barreras posibles, tiene todo lo relativo, por ejemplo, a lo que llamamos comercio móvil, o sea, la sustitución de las tarjetas de crédito por la portabilidad de números telefónicos, nos vamos a convertir en un número, nosotros somos el número telefónico que tengamos y ese número lo vamos a estar conservando, de tal manera que a través de todos los sistemas electrónicos, por ejemplo, si esto lo vemos en combinación con la etiqueta electrónica, pues, vamos a ir al supermercado, vamos a llenar el carrito, vamos a pasar por un arco electrónico y automáticamente se va a cargar la suma de todo lo que compramos, el total de lo que compramos a nuestra cuenta de teléfono, ya no necesitamos pasar tarjeta, ni mucho menos.

Incluso, llegando a un hotel seguramente vamos a tener un número al cual vamos a marcar en el hotel sin tener que pasar al mostrador y ahí directamente nos van a decir cuál es nuestra cuenta, cuál es el cuarto que tenemos asignado y vamos a recoger una tarjeta o alguna cosa así para entrar a la habitación. Toda esta parte electrónica pues significa datos de nosotros, domicilios, Registro Federal de Contribuyente, etc., en manos de un sinnúmero de corporaciones y de comercios.

¿Dónde van a quedar estos datos? ¿Qué va a pasar con estos datos?

La página de PROFECO, www.profeco.gob.mx contiene una sección de consumo informado, con énfasis en el comercio electrónico y en el Spam, áreas en las que los datos personales de los consumidores pueden ser fácilmente vulnerados, son explicados precisamente allí, en estas páginas de Internet.

Las alertas que saca continuamente PROFECO también son otro mecanismo que busca ayudar a la población para cuidar, entre otras cosas, sus datos personales.

Soluciones:

Desde la óptima internacional, primeramente, creo que PROFECO participa sobre todo en ejercicios internacionales a fin de conocer las mejores prácticas internacionales de la política pública de protección al consumidor y aquellos aspectos que están ligados a la protección de datos personales.

Verificación de sitios electrónicos, lo que llamamos *sweep days*, días de limpieza; análisis de los correos de Spam, de dónde vienen y las campañas internacionales de educación. Todo el asunto electrónico, sobre todo del Internet, si no hacemos acciones de tipo internacional, realmente no vamos a llegar a ningún lado, así de sencillo.

Existe consenso internacional de que el tratamiento ilegal de datos personales conduce a prácticas comerciales transfronterizas, engañosas y fraudulentas.

Algunas soluciones que alcanzamos a visualizar, desde la óptica internacional esencialmente:

Los países deberían de instrumentar, como mínimo, los lineamientos sobre protección de la privacidad y flujos transfronterizos de datos personales de la OCDE, de la Organización de Cooperación y Desarrollo Económico. Según la propia OCDE, el manejo de los datos personales debe de ser, primeramente, simple y tecnológicamente neutro, o sea, que se puedan utilizar diversas tecnologías, no estar sujetos únicamente a algún tipo de tecnología.

Se deben instrumentar esquemas de regulación o autorregulación o bien esquemas mixtos, que vean la parte de regulación desde los Gobiernos y una dosis de autorregulación.

Los sectores público y privado deben participar en el buen manejo de los datos personales en una sociedad.

Es muy importante dejar claro que este no es un asunto únicamente de incumbencia del gobierno, sino que tiene que haber necesariamente la participación de los particulares.

Conclusiones:

Es necesario generar una legislación nacional sobre la materia. Es una legislación realmente compleja, difícil, que incluso en estos momentos no está suficientemente discutida al interior del gobierno.

Hay diferentes líneas de política de protección de datos privados, ya que tenemos la línea europea sumamente constrictiva, precisamente en el traspaso de los datos personales y tenemos la línea americana, que es más permisiva, pero también con ciertos acotamientos.

Nos encontramos realmente en el momento de decisión de ver qué camino de esta bifurcación podemos tomar, si la línea de las políticas esencialmente norteamericanas o las políticas europeas, en relación a los datos personales.

Pero lo que sí es claro es que México requiere necesariamente de una legislación nacional sobre la materia. La posibilidad también de crear mercados de sociedades de información es importante, hay que verla también con esta perspectiva.

La exigibilidad, pues, de conductas específicas al respecto es necesaria y solamente se puede dar a través de la legislación.

Es muy importante la educación de los *ciber* usuarios especialmente y que los proveedores hagan del conocimiento de los consumidores cuál es su política de privacidad; o sea, la parte, como ya les comentaba, de responsabilidad por parte de las empresas.

Los consumidores confiarán más en la economía digital cuando se les garantice un uso adecuado y legal de sus datos personales. Esto de una manera muy rápida, ya que estamos muy constreñidos de tiempo, es lo que tenía preparado para ustedes en esta presentación.

Moderador: Alonso Gómez Robledo Verduzco: Comisionado del IFAI.

Antes de conceder la palabra a nuestros distinguidos invitados y especialistas en este tema, cuya importancia capital ya no puede escapar a nadie, permítaseme un muy breve, un muy pequeño prólogo a este mismo tema.

El pasado mes de septiembre se celebró en Montreux, Suiza, la XXVII Conferencia Internacional Sobre Protección de Datos y Vida Privada.

En esta importante conferencia internacional, se elaboró una declaración final, en donde se reconoció, entre otros muy relevantes puntos los siguientes, que quisiera destacar: Primero, se reconoció que el desarrollo de la sociedad de la información está dominado por la globalización del intercambio de información, y por el uso de tecnologías de procesamiento de datos con una injerencia cada día más peligrosa, cada día mayor y progresiva en el ámbito de la omnipresente vigilancia sobre las personas en todo el mundo.

Así como el hecho de que el rápido incremento del conocimiento en el campo de la genética podría convertir el ADN humano, nada más ni nada menos que en el dato personal más sensible de todos ellos.

Tercero, se reconoció que el derecho a la protección de datos y a la privacidad es un derecho humano fundamental. Así como una condición esencial en una sociedad democrática para asegurar las garantías individuales, un flujo libre de información y una economía de mercado abierta.

De igual suerte en esta declaración de Montreux se hace un formal y enfático llamado, y esto no es menor, a las Naciones Unidas, la ONU, para que prepare un instrumento jurídico vinculante que establezca en forma clara, así dice la declaración final, en forma clara y detallada los derechos a la protección de datos y la intimidad como derechos humanos de obligado cumplimiento.

Por otro lado, es ya un lugar común, pero no por común menos cierto sostener que el acceso a la información pública y la protección de datos personales constituyen los dos lados de una misma moneda.

Sin embargo y especialmente por este vertiginoso avance de la tecnología, los gobiernos mantienen cantidades masivas, creíblemente masivas de información personal sobre sus propios ciudadanos, declaraciones del impuesto sobre la renta, archivos de impuesto predial, gravámenes de títulos, archivos de asistencia social, registros de inmigración, registros de empleo y esto para sólo mencionar los más comunes y corrientes, digamos los más clásicos y tradicionales.

Aquí el acceso al público a tales registros en nombre del acceso a la información pública, a la información gubernamental podría, en algunos casos o en muchos, todo depende, podría privar al individuo de su capacidad, de su facultad para proteger su privacidad. En este sentido y en teoría, podrían concebirse como conceptos potencialmente opuestos por naturaleza.

Sin embargo el derecho positivo, la práctica internacional demuestra lo contrario y esto lo ha demostrado con creces. Se ha evidenciado que estos dos polos o caras de la moneda son bien compatibles. Esto es, son absolutamente conciliables en su aplicación.

Todo ello, y aquí quiero enfatizarlo, todo ello, y con esto termino, a condición que una ley sobre datos personales prevea mecanismos eficaces para la, digamos, no injerencia a la privacidad, a la par que prevea nítidamente que no se

entorpezca el libre flujo de información para el eficiente y óptimo funcionamiento de los mercados y la economía en general.

Sin más preámbulo quisiéramos dar la palabra a nuestros muy distinguidos invitados de esta mañana. Y si ustedes me permiten podríamos comenzar con la doctora María Alejandra Sepúlveda Toro. Directora Ejecutiva del Proyecto de Reforma y Modernización del Estado en Chile, ministerios de la Secretaría General de la Presidencia. Ella es abogada por la Universidad de Chile y tiene Master en Gerencia Pública y Diplomada en Dirección por Valores de la Universidad de Barcelona, España.

Ha sido docente en la Universidad de Magallanes, asesora jurídica en la Contraloría General de la República de Santiago y Contraloría Regional de Magallanes y Antártica Chilena. Igualmente Directora de Operaciones y Directora Nacional del Servicio del Registro Civil e Identificación.

Ponente: María Alejandra Sepúlveda Toro.

La protección de datos es una materia estrechamente vinculada al desarrollo de las tecnologías de la información y las comunicaciones y al proceso de globalización al que asisten todos nuestros países.

Es así como estamos reunidos entorno a la inquietud, a la necesidad de proteger los datos personales y entorno a los desafíos que esto plantea a nuestros distintos países.

Las declaraciones de la Antigua, de mayo 2003, de Santa Cruz de la Sierra, de noviembre 2003, de Cartagena de India, de mayo del 2004, han expresado que la protección de los datos personales constituye un derecho fundamental de las personas, relevándose las iniciativas regulatorias desarrolladas en los países iberoamericanos para proteger la privacidad de las personas y propender al acceso a la información y al control de sus datos que puedan hacer los ciudadanos.

Es importante destacar que estas materias se vinculan muy estrechamente con el desarrollo competitivo en nuestros países y con el bienestar social, especialmente de los sectores más postergados o más rezagados de nuestras comunidades.

El marco jurídico en Chile, lo vemos nosotros a partir de la Declaración Universal de los Derechos Humanos, del año 1948, en esta declaración se consagra el derecho a la intimidad y merece por primera vez un reconocimiento internacional. El artículo 12 de esta declaración dice que *nadie podrá ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia; ni de ataques a su honra o a su reputación*; estableciéndose que la ley debe brindar el amparo y la protección contra tales injerencias o ataques.

Desde entonces con mayor o menor desarrollo normativo los distintos tratados internaciones referidos a los derechos humanos han contemplado el derecho a la intimidad y de manera sistemática también ha sido recogido por las Cartas Fundamentales de nuestros Estados.

En Chile el artículo cinco de la Constitución Política del Estado, establece que la soberanía reside esencialmente en la nación y que su ejercicio reconoce como limitación el respeto a los derechos esenciales que emanan de la naturaleza humana y que es deber de los órganos del Estado respetar y promover tales derechos, que están garantizados por la constitución y por los tratados internacionales suscritos por Chile y que se encuentran vigentes.

Por su parte, el artículo 19 de la Constitución al tratar de las garantías individuales en su número cuatro, establece el respeto y la protección a la vida privada y la honra de la persona y su familia.

Y en el número cinco se establecen la inviolabilidad del hogar y la correspondencia.

La Ley 19,628, sobre protección de la vida privada, del año 1999, recoge todo lo anterior y su propósito es brindar una adecuada protección a la privacidad de las personas, reconociendo que ésta pertenece a la categoría de los derechos humanos y que los órganos del Estado están obligados a reconocerla y ampararla.

La ley fue publicada el día 28 de agosto de 1999 y lo que hace es regular el tratamiento de los datos personales contenidos en los registros o bancos de datos de los organismos públicos y privados.

La propia ley define lo que debemos entender por datos personales y dice que son los relativos a toda información concerniente a personas naturales identificadas o identificables.

La naturaleza jurídica de este derecho es sui géneris, pues no hay un derecho absoluto de dominio sobre la información por parte del titular, ya que éste puede adquirir un carácter de supraindividual, cuando el conocimiento de esa información sea necesaria para la protección de su titular o responda a fines superiores establecidos por el bien común.

También la ley define el dato sensible y dice que es aquel dato personal que se refiere a características físicas o morales de las personas o a hechos o circunstancias particulares de su vida privada o de su intimidad, tales como sus hábitos personales, sus creencias religiosas, sus opiniones políticas, su origen racial, los estados de salud físico psíquica y la vida sexual.

La fuente de los datos sensibles se encuentra en la propia Constitución, que ya he señalado y que se refiere a la protección de la vida privada de las personas de su familia.

El tratamiento de los datos personales. Este tratamiento sólo puede efectuarse cuando la Ley 19,628 lo autoriza. ¿Y cuándo lo autoriza esta ley? Cuando proviene de una fuente de acceso público, de registros públicos o privados de acceso no restringido a sus titulares.

También pueden tratarse estos datos cuando otras disposiciones legales lo permitan, como por ejemplo, el Código del Trabajo, que en materia de fiscalización permite el acceso a los registros de asistencia y de remuneraciones. Y finalmente lo permite cuando el titular consienta expresamente en ello.

El consentimiento del titular, de ser un consentimiento informado. Él debe conocer claramente la finalidad y el propósito del almacenamiento de sus datos y la posibilidad de que éstos sean dados a conocer a terceros. La autorización debe darse por escrito y la manera de revocarla es de la misma manera.

En cuanto al tratamiento de los datos sensibles, éstos no pueden ser objeto de tratamiento, salvo que la ley lo autorice, que exista consentimiento del titular o que sea necesario para la determinación o el otorgamiento de los beneficios de salud. Solamente en aquellos casos pueden ser tratados.

El tratamiento de los datos personales por los organismos públicos. Aquí se señala por la ley que esto sólo puede hacerse dentro de la competencia y de acuerdo con las normas de la propia ley.

Es decir, hay un tratamiento legal de los datos por parte de organismos públicos y la propia Ley 19,628 se encarga de definir quiénes son los organismos públicos, indicando que esto corresponde a los municipios, las intendencias, las gobernaciones, los servicios públicos y las empresas públicas, y que ellos, como son creados todos estos organismos por ley, siempre van a tener que enmarcar su actuar dentro de las competencias que la propia ley le establece.

Respecto de los datos personales relativos a condena y delitos por infracciones administrativas o faltas disciplinarios, sólo pueden comunicarse a los tribunales de justicia y a los otros organismos públicos, dentro del ámbito de su competencia, debiendo esto guardar reserva o secreto, según corresponda.

En general esta información no puede ser comunicada, una vez prescrita la acción penal o administrativa o cumplida la sanción o la pena, salvo en los casos en que los tribunales solicitasen esta información para la tramitación de sus asuntos que se encuentren pendientes.

El tratamiento de los datos por los organismos privados. En este caso pueden comunicar información de carácter económico, financiero, bancaria o comercial, cuando conste en letras de cambio, pagaré o cheques que hayan sido protestados o en el incumplimiento de mutuos hipotecarios, préstamos o créditos, sólo hasta cinco años después que la obligación se hizo exigible.

También debe cesar esta comunicación en el caso de que la obligación se haya pagado o se haya extinguido por cualquier otro modo legal. La excepción a esto es la información a los tribunales cuando esto lo requieran.

Aquí se excluyen todas las cuentas relativas a los consumos o servicios básicos, que son agua, luz, teléfono y gas. La ley contempla el recurso de la *Hábeas data*, como una acción sumarísima que da protección a los datos personales frente a un registro o a un banco de datos.

Los derechos amparados o la información, la modificación, la cancelación y el bloqueo de los datos, y las causales de procedencia son estas mismas cuando el titular de los datos haya solicitado esta información, y ésta no se le haya otorgado dentro de dos días o no haya sido denegada por el interés superior de la Nación.

Este es un proceso sumario que se inicia con la reclamación que hace el titular de los datos ante el Tribunal competente del domicilio del reclamado. En esta reclamación debe establecer la circunstancia de esta problemática que él está enfrentando, y acompañar los medios probatorios con los que cuenta.

De esta reclamación el Juez le da traslado al reclamado, que tiene el plazo de cinco días para hacer sus descargos, y también acompañar sus medios probatorios. Luego lo cual el tribunal puede abrir un término de prueba que tiene un plazo de cinco días, vencido el cual dentro del plazo de tres días debe dictar la sentencia definitiva, sentencia que es susceptible del recurso de apelación en ambos efectos, y para lo cual este Tribunal debe poner los antecedentes y conocimiento del Presidente de la Corte de Apelaciones respectiva, quien sin necesidad de que comparezcan las partes va a recibir estos antecedentes en cuenta y va a resolver en definitiva.

Contra estas sentencias no proceden los recursos de *casación*. Ahora, no puede ejercerse esta acción cuando entorpezca actividades fiscalizadoras de organismos que tienen como misión realizar esta fiscalización o afecta la seguridad de la Nación o el interés nacional. Esas son las limitaciones que tiene el *Hábeas data*.

Por otra parte, la ley crea un registro de bancos de datos personales a cargo de organismos públicos, señala que éste será de responsabilidades de servicio del Registro Civil e Identificación, y le da a este registro la característica de público, como una manera de hacerlo transparente para el ciudadano.

En este registro las bases de datos se informan por medios electrónicos y contiene un índice de los bancos de datos personales que están a cargo de los organismos públicos.

Las menciones que debe llevar este registro son: El nombre del banco de datos personales, el nombre de los organismos públicos que lo tienen a su cargo, el rol único tributario del organismo público, el fundamento jurídico de su existencia. Aquí volvemos nuevamente al principio de legalidad en cuanto al tratamiento de los datos, la finalidad del banco de datos, es decir, el objetivo de persigue, el tipo de datos almacenados y una descripción del universo de personas que éste contempla.

Sobre este registro, el Servicio de Registro Civil e Identificación, otorgará por medios electrónicos la información a todo aquel que la solicite, y de la manera, más rápida y transparente posible.

Esta es una visión panorámica del ordenamiento jurídico en Chile, teniendo en cuenta la importancia que esta materia reviste y de la preocupación que debemos mantener en torno a proteger los datos y a velar por el desarrollo eficiente, eficaz y ético de las tecnologías de información en nuestro país.

Moderador: Alonso Gómez Robledo Verduzco. Comisionado del IFAI.

La doctora Guillermina González Durán es egresada de la Facultad de Derecho de la Universidad Nacional Autónoma de México, de la UNAM; su experiencia profesional ha sido principalmente en la administración pública y en particular en el Instituto Nacional de Estadística, Geografía e Informática en el área de política informática; ha participado en el desarrollo de diversos proyectos normativos con instituciones como las Secretaría de Economía, de Gobernación, así como en el Cámara de Diputados en temas de firma electrónica, protección de datos personales y normas para la conservación de mensajes de datos; asimismo ha participado en la delegación mexicana en eventos internacionales relacionados con los temas antes mencionados; actualmente ocupa el cargo de Directora de Estándares y Nomenclaturas en la Dirección General de Coordinación de los Sistemas Nacionales, Estadísticos y de Información Geográfica del INEGI.

Ponente: Guillermina González Durán.

Quiero dividir mi presentación en tres grandes apartados:

El primero de ellos, hablar un poco del contexto y del ámbito de atribuciones del INEGI y el por qué de la participación en este tema.

En segundo tema las acciones que el INEGI realiza para proteger los datos que son obtenidos para fines estadísticos dentro de la institución y que son proporcionados por los informantes.

Y como tercer tema, quisiera hacer referencia a las acciones que está realizando el INEGI en cumplimiento de las disposiciones de la Ley Federal de Transparencia y Acceso a la Información Pública.

Como primer punto, quisiera mencionar, el INEGI tiene, dentro de sus atribuciones que le confiere la Ley de Información Estadística y Geográfica, dos grandes funciones.

Una de ellas es la integración de los sistemas nacionales, estadístico y de información geográfica. Y la otra es la de captar, producir, procesar y difundir información estadística y geográfica que pueda ser de interés general.

Para llevar a cabo estas funciones, el INEGI requiere de la participación de los informantes, mediante la obtención de datos que pueden y que tienen la finalidad de ser estadísticos.

En el contexto de la confidencialidad de los datos que el INEGI recaba para estos fines, la Ley de Información Estadística y Geográfica establece el derecho, en primer término, de la confidencialidad de los datos que son proporcionados; seguido, consagra el derecho de rectificación de los datos que le concierne a los informantes cuando exista algún error en ellos y, en su caso, de denunciar ante autoridad competente cuando no se respete la confidencialidad y reserva de dichos datos.

Asimismo, determina de una manera muy clara la finalidad para lo cual van a ser recabados los datos que son para fines estadísticos. Y que su divulgación únicamente podrá ser referida a tres unidades de observación con el propósito de no identificar de manera individual a la persona que proporcione los datos.

Otro artículo que hace referencia a la protección de datos es el artículo 40, que establece *el derecho que tienen las personas de solicitar ante autoridad competente que quede sin efecto la información que haya sido proporcionada mediante engaño o ilícitamente.*

Y finalmente contiene un apartado de infracciones que pueden ser imputables a servidores públicos, recolectores o censores que violen la confidencialidad de los datos que obtienen para los fines estadísticos.

Por su parte, el Reglamento de la Ley de Información Estadística establece qué debemos entender por dato estadístico confidencial y lo define como *los informes cualitativos y cuantitativos proporcionados por los informantes, para fines estadísticos referidos a una unidad de observación*.

En síntesis, los elementos de protección que establece la Ley de Información Estadística son los siguientes: El principio a la confidencialidad de los datos, el derecho a la rectificación de los datos que son proporcionados para dicho fin, la finalidad del uso de los datos, su difusión referida a un mínimo de tres unidades de información, el derecho que tiene el informante de solicitar que queden sin efecto cuando son proporcionados u obtenidos mediante engaño, infracciones imputables a las personas o servidores públicos que intervienen en la captación de información para fines estadísticos y la definición del dato estadístico como tal.

El segundo apartado en cuanto a los aspectos de confidencialidad previstos en los censos y encuestas del INEGI, se refiere a la protección de la información en las diferentes fases que son de captura, procesamiento y explotación del proceso de generación y actualización de información estadística y geográfica.

Para cada una de estas fases existen responsables del manejo de la información que en sus diferentes momentos tienen que hacerse cargo de preservar los derechos de confidencialidad.

Algunas de las acciones que se realizan para estos fines es, se elimina o suprime la información de carácter confidencial, datos que son traducidos a código numéricos que no permiten una identificación personal.

La información se presenta en diferentes niveles de desagregación a nivel país, estado, municipio, hombres, mujeres, sin que haya una identificación del nombre de la persona a la que se está refiriendo.

La confidencialidad aplica a los niveles más desagregados, a mayor detalle se agrupan mayor número de variables.

Desde el punto de vista del uso de las tecnologías de la información el INEGI tiene un programa integral de seguridad que contempla un sistema de prevención contra ataques internos y externos a la red. Esto es, a través de antivirus, antispam o el firewall, con esto se resguarda y se protege la integridad de la información que es contenida en bases de datos en las cuales se va integrando aquella información que finalmente va a tener un destino de información estadística o geográfica.

En cuanto a las acciones para el cumplimiento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el INEGI tiene la obligación de identificar y registrar ante el Instituto Federal de Acceso a la Información Pública los nombres de los sistemas utilizados, en cumplimiento de sus funciones, que contienen datos personales de los funcionarios públicos que laboran en la institución y de las personas físicas y morales que proporcionan sus datos.

Esto es, cuando las personas participan en su carácter de informantes, tienen la certeza de que sus datos no van a ser manejados de manera individual y que van a estar resguardados, desde el punto de vista tecnológico y desde el punto de vista también de la integridad de la información.

Esta información se encuentra disponible para todo el público en la Sección de Transparencia del INEGI en Internet, bajo el nombre Listado de Sistemas de Datos Personales del INEGI.

El INEGI lleva a cabo estas acciones con el Comité de Información del Instituto, a través de

la Unidad de Enlace del INEGI, que realiza las gestiones necesarias para garantizar el flujo de información entre el Instituto y los particulares.

A través de esta Unidad de Enlace se atienden solicitudes de información en los módulos de atención ciudadana del INEGI, que está diseminada en el país y que es atendida por los jefes estatales de atención a usuarios y comercialización.

Cuenta con un sistema de datos personales denominado Capital Humano, así como con varias listas de sistemas derivados de las encuestas que realiza, donde éstos se recaban y protegen, en donde existe un responsable del manejo de esta información.

Y, finalmente, el INEGI observa las políticas generales y procedimientos, para garantizar la protección de los datos personales publicados por el IFAI el 30 de septiembre del 2005. Se está realizando las acciones conducentes para llevar a cabo el cumplimiento de estas disposiciones.

En términos generales y de una manera muy breve, estas son las acciones que realiza el INEGI.

Quiero comentar, adicionalmente, que esta institución tiene un compromiso, desde hace varios años, cuando ejercía la función de política informática, de trabajar en los proyectos de protección de datos personales, en el contexto de lo que era la política informática dentro de la institución y que ahora continúa con este compromiso, a través de su responsabilidad de generador, producto y difusor de la información estadística y geográfica.

Moderador: Alonso Gómez Robledo Verduzco. Comisionado del IFAI.

El doctor Alfredo Chirino Sánchez es profesor catedrático de Derecho Penal, de la Facultad de Derecho de la Universidad de Costa Rica. Obtuvo su Maestría y Doctorado en Derecho en la Universidad de Joan Wolfart Gate de Frankfurt, en la República Federal de Alemania. Ha publicado numerosos artículos, ensayos y libros sobre temas de Derecho Penal, Procesal Penal, de Derecho Constitucional y sobre el Derecho a la Protección de la Persona frente al Tratamiento de sus Datos. Entre ellos podríamos mencionar los siguientes: El Derecho a información y la Administración de Justicia en América Latina; Informática y Derecho a la Intimidad; Perspectivas de Política Criminal; El Derecho a la Información y el Papel de las Instituciones del Sector de Justicia.

Ponente: Eric Alfredo Chirino Sánchez.

Muchas gracias. Muy buenos días a todos y a todas, distinguidos y distinguidas miembros de este presidium, y compañeros, compañeras y colegas todos preocupados por el problema de la protección de datos.

Antes que nada agradecer a los organizadores y copatrocinadores de este evento, no sólo por la capacidad de convocatoria que han tenido para que este tema se localice en muy alta, la jerarquía de los temas que preocupan a México, como también por darnos la posibilidad a la Red Iberoamérica de Protección de Datos Personales, tener la ocasión de hacer este IV Encuentro, que como lo decía nuestro Director, indudablemente marcará un hito, donde se hablará de un antes y un después de este IV Encuentro que estamos realizando.

No quería hacer una presentación donde hablara exclusivamente de mi país, quería, más que todo, compartir con ustedes algunos problemas que probablemente nos tienen unidos a todos los países de América Latina, y que nos presentan hoy en día una dificultad enorme para poder superar los déficit de orden legislativo y cultural que actualmente tienen el desarrollo de la protección de datos sometida a una grave situación espiritual. Si me permiten ustedes usar esa palabra.

Principalmente quería comenzar con una proposición. La proposición es: ¿Realmente será el problema de la protección de datos en manos del Estado un problema del Estado de derecho? Y quiero con esa proposición que les va a parecer

a ustedes paradójica comenzar diciendo que en efecto nadie va a dudar que el Estado, el gobierno, los gobiernos, las administraciones públicas tengan necesidad de un procesamiento intenso de datos personales.

Esto es evidente en la administración tributaria, es evidente en la administración de justicia penal, es evidente también a la hora de tomar decisiones de carácter público en el sector salud, en el sector financiero, en el sector comercial.

Así que no hay duda de que el Estado tiene necesidad del tratamiento de datos personales, tiene necesidad también de ingresar a los bancos de datos privados que existen, y tiene necesidad intensa de un desarrollo muy fuerte de bancos de datos.

Pero también tiene necesidad y urgencia, y también mucha voracidad por entrar a los bancos de datos privados, que en este momento conservan enormes cantidades de datos personales, que incluso se almacenas a beneficio de inventario.

Es decir, se van manteniendo ahí embodegados para algún día ser útiles para algún fin estatal, que hoy no conocemos.

Este tráfico de informaciones tiene riesgos y tiene posibilidades. Quizá el riesgo más importante, y quizá la trascendencia más grande que tiene es ofrecernos un doble juego de posibilidades. Parece que este monto hace realidad aquella idea de que el infierno son los otros, la posibilidad de que los otros sepan más de nosotros que es una realidad hoy muy fuerte.

Y en una democracia el intercambio o el flujo de información es hoy quizá la esencia material de un nuevo concepto de democracia.

Hemos estado demasiado acostumbrados a que nuestro concepto de democracia se basa en el ejercicio de facultades cívicas y electorales. La democracia de la sociedad a la información es una democracia de flujos de informaciones y eso cambia y dinamiza totalmente la operación de la gestión pública.

La minería de datos, el phishing que se planteaba hoy en la conferencia magistral que recibimos en la mañana por parte del doctor Carlos Arce, así como también la posibilidad de usar software robots que ya se anuncian también por parte de la administración tributaria para mediante los mecanismos de minería de datos poder recopilar, digámoslo así, la gestión cotidiana de un ciudadano para saber si efectivamente su pago de tarjeta de crédito coincide con lo que está pagando de impuestos, refleja de alguna manera los enormes retos a los cuales estamos refiriéndonos.

La doctora Sepúlveda Toro nos indicaba cómo la legislación chilena está en este momento poniendo un especial énfasis en una definición de datos personales. Yo creo que esa es una preocupación que también deberíamos de seguir el resto de los países de la región, ya que en este momento si hay algo que es distinto de país a país es cómo definimos el dato personal.

La información referida en la persona identificada o identificable que parece muy cercana a la definición que viene en la legislación federal de protección de de datos personales de la República Federal de Alemania, parece ser una buena opción y parece que los chilenos han decido orientar su construcción normativa a partir de eso.

Pero también está la preocupación de que la definición de datos personales puede variar en los países federales, según las legislaciones de cada estado, de cada provincia decidan apartarse de ese concepto. Lo que va a generar para las administraciones públicas, sobre todo, en estados federales como el de México, la posibilidad de que se puedan crear oasis o paraísos del procesamiento de datos donde ese régimen o donde el estándar legislativo sea menor al que ya incluso se pudiera tener a un nivel federal.

Ese riesgo enorme es parte de ese juego de espejos, ese juego de doble posibilidad que tienen las regulaciones de protección de datos.

Indudablemente entre los basamentos para el reconocimiento de la tutela de la protección de datos está precisamente en darles a las personas la posibilidad de autodeterminarse.

En la primera sesión, en la conferencia inicial se presentaron importantes cuestionamientos sobre la definición del llamado derecho fundamental a la protección de datos como un derecho autónomo, porque efectivamente esa doctrina traducida a los términos latinoamericanos es realmente difícil de entender, precisamente porque nosotros estamos en este momento construyendo el derecho de protección de datos sobre una construcción realmente antojadiza, un poco procesal y demasiado formalista como es el Hábeas data.

En América Latina hablar de protección de datos significa hablar de Hábeas data, y ese es quizá una de las anclas más pesas con las cuales tenemos que luchar cotidianamente para tratar de construir un sistema de protección de datos que sea realmente razonable; porque el Hábeas data funciona cuando ya nada se puede hacer, ya cuando el daño está hecho y los ciudadanos han sufrido lesiones en su capacidad de definir quién, cuándo, dónde y bajo qué circunstancias tiene acceso a sus datos personales.

Y si el derecho protegido no es realmente un derecho fundamental, si no un derecho procesal, evidentemente vamos a recibir de parte de las legislaturas, de parte de quienes tienen que decidir nuestros destinos, una evidente moneda de difícil compra como es el Hábeas data.

Por eso quisiera que mi primer mensaje de esta exposición sea el de decirles que hay que tener mucho cuidado cuando ponemos todas nuestras cartas a favor de la Hábeas data y dejamos sin posibilidad a una regulación que además de darnos y reconocernos la posibilidad de autodeterminarnos y de respetar nuestra dignidad humana, además nos permita prevenir los riesgos de un procesamiento de datos intenso.

Me parece trascendental decir que las circunstancias del modo, el tiempo y el lugar en que se está dando el tráfico de datos en materia de intimidad, tiene que ver también con la gestión del Estado.

Nos recordaba la compañera Guillermina a la hora de referirse a la anonimidad y seudoanonimidad de los datos estadísticos de que efectivamente si no hubiera una reflexión del Estado por pensar si efectivamente anonimizando los datos le concedemos a la personas la posibilidad de un tráfico más o menos lícito dentro de la sociedad, probablemente la preocupación dentro de nuestras colectividades no se generaría. Lo que quiero decir es que no todo es negativo desde el punto de vista, la visión de la protección de datos en manos del Estado.

Probablemente esa reflexión algún día construya una cultura de protección de datos.

Quizá los colegas que vienen de Europa y que están entre nosotros poco a poco han ido comprendiendo la extraña diferencia de discurso entre ellos y nosotros, la diferencia es cultural.

En un país como la República Federal de Alemania, desde la época de la Segunda Guerra Mundial donde a través de tarjetas perforadas se hizo un censo detallado de quienes eran judíos, quiénes eran homosexuales, quiénes eran aquellos que eran extraños a la comunidad y eficientemente se fueron cartografiando las sociedad para determinar esos grupos y producir un genocidio más eficiente, indudablemente tiene que generar una sensibilidad muy grande por quién tiene los datos y para qué los tiene.

En esa sociedad, en mi país muy concretamente, no puedo hablar por todos, pero mi país es muy peculiar en eso, la idea de que alguien proteja su intimidad es porque algo quiere ocultar.

Nosotros partimos de la idea de que Dios está en la casa de todos, pero cada uno tiene en su casa un castillo y la idea de la protección de la intimidad está íntimamente ligada a protección de la propiedad privada.

Esa patrimonialización del concepto de intimidad que es muy pequeño burgués y podríamos decir decimonónico choca directamente con un derecho fundamental como éste que pretende realizar una condición de derecho fundamental nuevo, algunos dicen de tercera generación, en donde lo esencial no es exactamente la intimidad, sino la capacidad de ser ciudadanos en un mundo que hace tiempo se ha objetivizado profundamente a través del proceso informativo.

Es por eso que surge el derecho a la autodeterminación informativa y yo quisiera postularlo para la discusión, quisiera dejar un problema en el auditorio para que esto genere un poco de emoción y violencia, que siempre es importante en un evento como éste.

Y sugerir que probablemente el bien jurídico tutelado en las futuras legislaciones sobre protección de datos, incluso también en aquella proyectada en México, tienen como centro no la privacidad en la intimidad, sino la otra contra-cara de la moneda, el reservo de la moneda, el problema del acceso a la información pública y me refiero precisamente a ese derecho con esa palabra tan poco probable para la Real Academia de la Lengua que es el derecho a la autodeterminación informativa, que es una reconstrucción del vocablo alemán, pero que hace referencia a los dos aspectos que yo quisiera rescatar de otras exposiciones que nos han precedido, que es precisamente la reflexión de por qué es tan misterioso la vinculación entre la protección de datos y la dignidad y los derechos humanos.

Precisamente porque la Hábeas data es sólo protección procesal, porque la teoría de las esferas en materia de protección de los derechos, sobre todo de la primera generación ha hecho aguas, como lo demostró Jürgen Habermas en aquel libro *Facticidad y validez*, quien sigue teniendo una enorme vigencia para la discusión de derechos humanos tanto en Europa, como en América, y porque efectivamente podemos estar hablando de un tratamiento de datos en manos del Estado que no necesariamente es sensitivo a los datos de las personas. Este derecho cobra una especial importancia para la discusión de América Latina.

Yo quisiera ver que efectivamente la autodeterminación informativa sea una respuesta al problema que estamos planteando, ¿pero cómo lo podría ser? En este momento yo creo que son tres los principios de la protección de datos que no están siendo considerados a la hora de construir las políticas estatales de manejo de información y lo voy a decir de manera genérica sin conocer por supuesto el detalle de la discusión y del tipo de gestión de las administraciones públicas en México, pero casi podría decir que como tesis de principio son tres los que están probablemente en discusión: El principio de sujeción a los fines del procesamiento de datos; el principio de proporcionalidad en el sentido de reducir y referir el procesamiento de datos sólo a aquellos datos que sean indispensables y necesarios para la gestión pública y el tercero, el más importante, el principio de consentimiento y transparencia.

Y me refiero a esos tres principios, porque si el derecho a la autodeterminación informativa realmente tiene alguna capacidad de ser respuesta a los problemas que estamos viviendo en el momento histórico que trasunta América Latina, es precisamente el tratar de darle vigencia a esos tres principios.

¿Por qué? Porque esos tres principios tienen que ver con la parte de la protección de datos que quiere ser preventiva, quiere ser tuteladora y quiere ser garantizadora. Son las tres cosas que no hace el *Hábeas data*, que funciona cuando ya todo está perdido, cuando ya no puedo salvar nada.

Si yo realmente pongo el énfasis de la discusión pública sobre cómo los ciudadanos pueden

defender sus posiciones jurídicas frente a un Estado urgido de informaciones, urgido de identificar a los ciudadanos. Lo decía nuestro moderador al inicio de esta exposición, que las declaraciones de Montreux van dirigidas directamente a poner el dedo en llaga en los datos genéticos y biométricos.

Hoy estamos discutiendo en nuestros países la posibilidad de usar chips, para identificar a los ejecutivos de altas empresas y así evitar el secuestro.

Estamos estableciendo la capacidad de ponerle a nuestros vehículos sistemas de protección satelital para el robo de vehículos, y la posibilidad de vigilar a los ciudadanos, con el efecto de evitar que sean secuestrados, pero también de que se conviertan en delincuentes.

Si esas tres visiones que están, obviamente, aderezadas de la discusión de seguridad, que en este momento preocupa muy alto en la jerarquía de valores de casi todos nuestros países, como uno de los problemas sociales más importantes, nos damos cuenta que estos tres principios de la protección de datos pierden valor, porque cualquier cosa que garantice seguridad no merece ninguna defensa de ningún derecho fundamental, mucho menos del derecho a la protección de datos, el cual llega tarde a América Latina y llega como la coyuntura cuando aún en algún momento se vio como una opción democrática.

Yo quisiera, además, decirles que me parece muy casual y muy importante que sea el Instituto Federal de Acceso a la Información Pública quien se haya convertido en un actor importante dentro de México, para discutir y analizar también el tema de la protección de datos.

Y no dudo que este derecho de acceso a la información está en una relación de tensión con el derecho a la protección de datos personales y que probablemente los colegas doctrinistas del Derecho Público y Constitucional en México, como lo han dicho en otras regiones, dicen que la única posibilidad de que este Derecho sobreviva es llevarlo a una concordancia práctica. Claro, el secreto está en no decir cómo se logra esa concordancia práctica.

Pero yo tampoco voy a contestar esa pregunta, probablemente lo podemos dejar para la discusión. Pero lo que yo sí quisiera decirles es que no es contradictorio que esos dos derechos sobrevivan juntos en la democracia y que vivan para darle a la democracia un nuevo momento, precisamente porque son dos caras de la misma moneda.

En Europa el Derecho al Acceso a la Información Pública, sobre todo en los países que tuvieron leyes de protección de datos, como lo fue el caso de la República Federal de Alemania, llegó tarde y de la mano de la protección del ambiente. En los países nórdicos se tiene desde hace muchos años el Derecho de Acceso a la Información.

La pregunta es: ¿Por qué llegan los dos juntos a América Latina?, cuando nuestra preocupación de que nuestra casa es nuestro castillo, y si el que nada tiene que ocultar nada tiene que temer, tengan ahora que defender una nueva visión cultural sobre este derecho.

Los principios que orientan esta protección ya los ha analizado en su vinculación jurídica, tanto doña Alejandra como doña Guillermina. Así que voy a obviar la discusión sobre eso y voy a pasar la siguiente transparencia.

La situación espiritual en la que vivimos es que no tenemos el derecho a la autodeterminación informativa, no hay leyes de protección de datos, entonces, ¿qué sucede? Como lo planteaba la colega Karin Kuhfeldt Salazar, que nos refería cómo en Colombia la evolución ha sido casi únicamente jurisprudencial y de la mano de las acciones de tutela y de un *Hábeas data* tan limitado como el nuestro en nuestro país, efectivamente demuestran que la única opción que tienen los ciudadanos hoy en día a falta de una ley de protección de datos es precisamente una tutela jurisdiccional.

Si ustedes dan una mirada al desarrollo jurisprudencial de mi país, se van a dar cuenta que la preocupación ha sido precisamente por donde no urge todavía los datos de las administraciones públicas, sino concretamente en el tema de seguridad.

Los datos que se van inscribiendo en los registros criminales. Esos son los que han dado origen a toda la preocupación de datos en mi país, y hoy últimamente al problema del acceso a los datos comerciales, a los datos de carácter financiero.

Últimamente la jurisprudencia de la Sala Constitucional de mi país ha ido evolucionando con le objetivo de dar al derecho de la autodeterminación informativa más poderes.

Hace un par de semanas se notificó la sentencia que todavía no tiene redacción, pero tenemos el por tanto, en donde se obliga a las empresas protectoras de crédito, a mantener un derecho del olvido de los registros financieros de un plazo máximo de cuatro años.

Donde no existían límites, ahora hay un plazo de cuatro años, y efectivamente esto le ha creado a las empresas protectoras de crédito una difícil situación de sobrevivencia económica, porque ahora sí tienen que hacer calidad de datos.

La protección de la integridad de los datos, de la precisión de los datos, de la exactitud de los datos, y sobre todo, lo más importante, de olvidar los datos cuando éstos carecen ya de interés y/o devolverle la vida civil a buena parte de los deudores en mi país. Esto nos lleva a que la oferta de una tutela administrativa del derecho a la autodeterminación informativa quede en manos de reglamentos.

Yo quisiera decirles que el derecho a la autodeterminación informativa requiere siempre regulación legal. El principio más importante, y lo hacia ver la doctora Alejandra Sepúlveda, es que el tema de la protección de datos sólo puede ser regulada vía legal. Cualquier decisión reglamentaria o de control administrativo de la protección de datos carecería del valor necesario para regular, limitar y restringir un derecho fundamental.

Quiero concluir esta reflexión, que ha querido ser una reflexión global y no exclusivamente nacional, dando tres mensajes que me parece que pueden ser importantes como himnos de batalla en la discusión que vamos a tener en los próximos años en América Latina, sobre el derecho a la autodeterminación informativa. Primero, que no importa cómo le pongamos de nombre al bien jurídico tutelado.

Lo evidente y lo trascendental en la protección y la discusión sobre la protección de datos personales es cuál es la definición de datos personales que vamos a usar.

Segundo, olvidemos totalmente cuál puede ser la reflexión sobre datos sensibles. Lo que hoy parece ser no sensible lo será mañana. Ese no parece ser el camino adecuado, como lo decía, Stefano Rodotá hace muchos años. Probablemente la preocupación sobre la sensibilidad de los datos no parecer ser la fuente de análisis esencial para la discusión sobre protección de datos, si no precisamente la idea del control del flujo de informaciones sea la forma más excelente de poder discutir con algún grado de racionalidad democrático el avance en el derecho de la protección de datos.

Y el tercer mensaje que quería transmitirles, es que hoy ya tienen un manejo masivo de datos en manos del Estado, no sólo los estadísticos, probablemente la administración tributaria como lo hacía ver nuestro conferencista magistral de hoy en la mañana, también en materia de derecho del consumidor, de datos financieros, de datos relacionados con la actividad electoral de los ciudadanos y ciudadanas y por supuesto, todos los datos referidos a la administración de justicia.

Así es que ese volumen de datos ya demuestra la necesidad de un derecho de protección de datos regulado vía legal y la única esperanza que tiene América Latina es la de avanzar hasta la

ocasión y la oportunidad de tener leyes que permitan desarrollar después una cultura de protección de datos.

Ya no tenemos tiempo de desarrollar la cultura antes de la ley, démosle la oportunidad a la ley de crear la cultura.

Moderador: Alonso Gómez Roble Verduzco. Comisionado del IFAI.

Solicito la participación del doctor Andrés Albo Márquez; quien tomó posesión como Consejero del Instituto Federal Electoral el 3 de noviembre de 2003; es licenciado en Ciencias Sociales por el Instituto Tecnológico Autónomo de México, Maestro en Ciencias Sociales y Ciencia Política por la Universidad de Siracusa; tiene estudios de postgrado por la Universidad de George Washington, D. C.; hasta octubre del 2003 fue director del Departamento de Estudios Sociopolíticos de Banamex; en 1994 fue observador electoral en México en los comicios federales y realizó actividades en esa materia en 1991; asimismo fungió como consejero en el Consejo Local del Instituto Electoral del Distrito Federal en los años de 1997, 2000 y 2003, en el proceso de 1997 incluyó la calificación del primer Jefe de Gobierno del Distrito Federal; igualmente fue coordinador del Anuario Estadístico México Social-Banamex y de elecciones locales y elecciones nacionales 1970-2000; cabe mencionar que ha sido profesor del ITAM y de la Universidad Iberoamericana.

Ponente: Andrés Albo Márquez.

Este tipo de eventos son necesarios para profundizar el debate en torno a la cultura de la transparencia, que no se puede entender sin lo que en mi concepto es su lado complementario, que es el tratamiento y protección de los datos personales, ya se decía que es la otra cara de la moneda.

El motivo de mi intervención es compartir la experiencia del Instituto Federal Electoral en la materia. Para el IFE existe, digamos, en una gran definición, dos ámbitos de manejo de datos personales.

El primero y desde luego más significativo es el del padrón electoral.

Y el segundo más limitado, pero crecientemente relevante y demandado por los ciudadanos es la información de datos personales vinculados a la actividad de los partidos políticos.

Antes de entrar al tema permítanme robarles nada más dos minutos para hacer algunas reflexiones sobre la importancia y uso de la información confidencial desde la óptica de la institución pública y autónoma como es el IFE.

¿Hay que delimitar la información pública de la reservada o confidencial?, depende en estricto sentido de su naturaleza.

En los últimos años hemos sido testigos del avance de dos movimientos de alcance mundial, el primero, desde luego más vigoroso y extendido ha sido la transparencia; el segundo, en el lado opuesto y con un avance posterior, pero crecientemente importante ha sido la información confidencial.

Así nos encontramos con que la transparencia de la información gubernamental es hoy una realidad, incluso hay plena aceptación de que la secrecía de la información del gobierno es incompatible con las democracias modernas.

Del lado opuesto o para ser más precisos, si me permiten la metáfora de forma recíproca a la apertura, encontramos la información confidencial, y yendo al grano, podemos hablar de la responsabilidad que tiene el gobierno de proteger los datos personales que los individuos le entregan con propósitos específicos, por medio de las leyes el Estado determina la frontera entre lo público y lo privado, de forma que éste debe garantizar el ejercicio de los derechos individuales, proteger la intimidad y evitar que la información personal se haga pública.

La protección de este derecho salvaguarda la voluntad de mantener fuera del conocimiento público aspectos de la vida personal tales como

la convivencia familiar, la conducta sexual y afectiva, las creencias religiosas, el patrimonio personal, entre otros.

Vale decir que tanto el ordenamiento jurídico internacional, como el mexicano han previsto disposiciones que tienen por objeto la defensa y protección de la vida privada, no entro al detalle del marco jurídico en México, ya lo expuso con toda precisión Carlos Arce, y seguramente mejor de lo que yo podría hacerlo.

Lo que quisiera es concentrarme, si me lo permiten, en el Registro Federal de Electores; éste, sin duda, es la base de datos más importante que maneja el Instituto y su relevancia es nacional y rebasa por mucho el ámbito estrictamente electoral.

Hablamos de un banco de datos con información como nombre, sexo, edad, domicilio, clave de elector y que acumula datos de más de 70, casi 75 millones de empadronados.

Por la importancia del padrón electoral su protección y trámite se regula conforme a lo dispuesto por el COFIPE, el Código Federal de Instituciones y Procedimientos Electorales, es la excepción de la norma del manejo del padrón electoral, es la excepción de la norma establecida en el reglamento propio del Instituto, en el reglamento de transparencia en materia de datos electorales.

Menciono algunas características que definen el tratamiento de este banco de datos personales, pero que tiene las características precisas de ser un banco también electoral; combina, por un lado, una característica de lo electoral y junto de un banco de datos para la identificación de los ciudadanos.

La primera característica que define el COFIPE es que los partidos, los integrantes de los consejos a nivel general, local y distrital, así como los miembros de las llamadas Comisiones de Vigilancia que son órganos creados ex profesos para vigilar la conformación y veracidad del banco de datos, tienen acceso irrestricto a todos los datos que conforman el padrón electoral y la lista nominal para efectos de control y revisión.

Por contra, el acceso a la base de datos se encuentra totalmente restringido para aquellos funcionarios que no tengan vinculación con su manejo.

El Registro cuenta con una plataforma tecnológica que registra electrónicamente cualquier consulta realidad por funcionarios o personal acreditado para efectos de cualquier control.

Por tal motivo se puede tener plena certeza que un mal manejo de dicha información implicaría, entre otras cosas, una posible responsabilidad administrativa. Desafortunadamente hace algunos meses vivimos esta triste experiencia.

Otra característica relevante es que, de acuerdo con el Código Electoral, el Instituto está obligado a compartir la información del padrón con la Secretaría de Gobernación mediante, desde luego, la celebración de convenios.

Asimismo, el Registro Federal de Electores se encuentra obligado a proporcionar información confidencial en juicios, recursos o procedimientos en que el IFE fuere parte o bien por un mandato de lo que la ley señala, como juez competente.

El Instituto ha interpretado que el concepto juez competente es aplicable exclusivamente a los funcionarios del Poder Judicial y a las autoridades administrativas, que estén tramitando asuntos de orden legal y se excluye a los ministerios públicos locales, federales o a los tribunales administrativos.

De esta forma se garantiza que la información personal que maneja el IFE sólo será conocida por un grupo reducidísimo de gente que tienen acceso a éste, con fines exclusivos de supervisión electoral. Y, por tanto, se puede concluir que la regulación del manejo de datos electoral obedece a la particularidad y objetivos del padrón, y además de servir de insumo para emitir

la credencial electoral con fotografía que sirve, hay que recordarlo, como el instrumento para ejercer el voto y, desde luego, como una cédula en el uso común de identidad nacional.

A la par de la regulación que establece el COFIPE en materia de datos personales, hago mención que en junio pasado el Instituto aprobó un nuevo Reglamento de Transparencia, que incluye, de manera destacada, un apartado correspondiente a datos personales.

Resalto cuatro aspectos relevantes para el tema que hoy nos ocupa. Primero, establece este Reglamento, con toda claridad, que los datos personales son información de carácter confidencial y, desde luego, las definiciones alrededor de esto.

Su difusión, distribución y comercialización debe apegarse estrictamente a las disposiciones que se señalan en este Reglamento.

Segundo. Se incorpora un apartado de responsabilidades para los servidores públicos, con lo cual se obliga a mantener la confidencialidad de los documentos, además de precisar las consecuencias de uso indebido para la información reservada o confidencial.

Tercero. Con la nueva regulación se garantiza la apertura de la información pública, sin comprometer datos, que son patrimonio exclusivo de los ciudadanos.

Finalmente se posibilita al ciudadano mecanismos de acceso y corrección de sus propios datos, y define los principios que permiten la protección de información confidencial.

Me ocuparé ahora de la información, de los datos personales vinculados a las actividades de los partidos políticos.

Las finanzas de los partidos son asuntos de interés público. Por ello utilizo dos ejemplos significativos en materia de fiscalización, que involucran el manejo de datos personales.

Son casos complejos que buscan el equilibrio entre la necesidad de hacer información pública, relacionada con manejo de recursos, que en su mayoría, más del 90 por ciento son recursos, dineros públicos y la obligación de salvaguardar la información confidencial de personas vinculadas con las actividades de los partidos.

El primer ejemplo que quisiera señalar se refiere al Acuerdo que aprobó la Comisión de Fiscalización para publicar en la página de Internet del Instituto, la información sobre el monto total de las aportaciones que reciben los partidos y el nombre de los aportantes. Esto como un esfuerzo de rendición de cuentas de los ingresos que obtienen los partidos políticos por medio de sus simpatizantes.

Este acuerdo da a conocer el nombre y el monto aportado, pero mantiene la confidencialidad de otros datos personales.

Un segundo ejemplo da cuenta de las medidas que tomó también la Comisión de Fiscalización para diversificar mecanismos de autofinanciamiento, esto hace apenas hace unas semanas.

Sí, efectivamente recientemente se aprueba el Acuerdo que establece las modalidades y criterios para la utilización de los números telefónicos 01-800 y 01-900, como medio para recaudar fondos por la vía de aportaciones de militantes y simpatizantes.

Esta medida tiene un doble valor o factor benéfico. Por una parte permite que los partidos se alleguen de recursos de manera expedita y absolutamente transparente. Y por otra, se tiene certeza sobre la legalidad del origen de los recursos obtenidos, pues las aportaciones se deben realizar por medios de tarjetas bancarias de los aportantes, y los depósitos se deben hacer directamente a las cuentas que para tal propósito apertura el partido. Ambos mecanismos provén de evidencias confiables de los movimientos bancarios.

Tanto para el caso de las aportaciones realizadas por medio de depósitos, como por la vía telefónica, resulta relevante insistir en que de ningún modo se pone en riesgo la identidad o la situación patrimonial del aportante, pero la autoridad tiene plena certeza del origen lícito de los recursos.

El IFE es cuidadoso al revelar únicamente la información sobre el nombre del aportante y el monto de la contribución. Todos los ciudadanos sabrán esta información. Y de esta forma se garantiza la privacidad de otros datos personales al omitir información como domicilio, clave de elector, número telefónico o alguna otra información bancaria.

Para concluir mi intervención quisiera hacer énfasis en que el reconocimiento legal del derecho a la protección de datos personales es un elemento esencial en la vida de las democracias. A partir de este tipo de acciones se puede distinguir el espacio público del privado.

La protección a la vida privada es necesaria para garantizar el respeto a la dignidad personal, y desde mi perspectiva existe un doble propósito en la protección de la intimidad. Por una parte se trata de asegurar la libertad individual, y por otra, se intenta restringir o prohibir el uso indebido de información confidencial.

El Instituto Federal Electoral es consciente de esta responsabilidad, por ello desarrolla acciones como las que he mencionado para delimitar la frontera entre la información pública relacionada con el funcionamiento del Instituto y los partidos políticos, y de aquella información que es confidencial y que le entregan los ciudadanos para el cumplimiento de sus objetivos y atribuciones legales.

Moderador: Alonso Gómez Robledo Verduzco. Comisionado del IFAI.

La intervención estará a cargo del licenciado Andrés Calero Aguilar, egresado de la Universidad Panamericana y con estudios de especialidad en el Instituto Nacional de Administración Pública, el Instituto Tecnológico Autónomo de México y la misma Universidad Iberoamericana.

En el campo laboral ha trabajado en diversas dependencias del sector público, como es la Secretaría de Relaciones Exteriores y el Instituto Mexicano de la Radio.

Inició su labor en al Comisión Nacional de los Derechos Humanos en agosto de 1990, ocupando una jefatura de departamento y ha laborado por un lapso de más de 10 años teniendo actualmente el honroso cargo de Tercer Visitador General.

Ponente: Andrés Calero Aguilar.

Quiero compartir la experiencia esta mañana de la Comisión Nacional de los Derechos Humanos en materia de protección de datos personales y refiriendo un poco a las ideas planteas por el doctor Chirino, de la concordancia práctica entre el derecho a la información y el derecho a la protección de datos personales con algunos ejemplos que hemos tenido en el seno del ombudsman nacional.

La CNDH en su carácter de órgano constitucional autónomo y por lo tanto sujeto obligado de las disposiciones de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental ha realizado una serie de acciones en materia de acceso a la información y protección de datos personales:

1.- La normatividad de la Comisión Nacional de Derechos Humanos en materia de datos personales.

Reconociendo la importancia de que las personas tengan conocimiento de la información que de ellos obra en la Comisión Nacional y con la finalidad de que hagan uso de su derecho de acceso y corrección de los datos personales.

En primer término en la Comisión Nacional de Derechos Humanos se realizó el proyecto de normatividad en el que se establecen los

órganos, criterios y procedimientos institucionales para proporcionar a particulares el acceso tanto a los datos personales, como a la información en posesión del ombudsman nacional.

Una vez elaborado dicho proyecto, el Consejo Consultivo de la Comisión Nacional de Derechos Humanos en su sesión ordinaria número 174, celebrada el 8 de abril del 2003 emitió el Reglamento de Transparencia y Acceso a la Información de la Comisión Nacional de Derechos Humanos, mismo que fue publicado en el Diario Oficial de la Federación el 29 de abril del 2003.

El Título Tercero de este Reglamento se refiere a la protección de datos personales y, dentro de las disposiciones más importantes establecidas en dicho apartado se encuentran las siguientes:

En el caso de las solicitudes de datos que obren en un sistema de datos personales, sólo los titulares de los mismos o sus representes podrán, previa acreditación, solicitar a la Unidad de Enlace se les proporcionen los datos que obren en un sistema de datos personales.

La Unidad de Enlace deberá entregarle al solicitante en un plazo de 10 hábiles contados desde la fecha en que se presentó la solicitud, la información o bien la respuesta que al respecto remite el área responsable.

Por lo que se refiere a las solicitudes de modificación de los datos, los titulares de éstos o sus representantes podrán solicitar, previa acreditación ante la Unidad de Enlace, que se modifiquen los datos que obran en cualquier sistema de datos personales.

El titular deberá entregar una solicitud en la que se señale el sistema de datos personales, indiquen las modificaciones que deban realizarse y aporten la documentación que motive su petición.

La Unidad de Enlace deberá entregar al solicitante en un plazo de 30 días hábiles, contados desde la fecha en que presentó la solicitud, la comunicación por medio de la cual el área responsable haga constar las modificaciones o bien, informe de manera fundada y motivada las razones por las cuales no procedió lo solicitado.

Contra la negativa de entrega o corrección de estos datos personales, así como la falta de respuesta en los términos que se establecieron en los dos supuestos anteriores, procede el recurso de revisión al que se refiere el propio Reglamento de la Comisión Nacional de Derechos Humanos.

Con posterioridad, en concordancia con lo establecido en el artículo 20 de la Ley Federal de Transparencia, en agosto de 2003 se elaboró el procedimiento para la atención de las solicitudes de acceso y corrección de datos personales que se reciben por escrito en la Comisión Nacional en el cual se plasman las disposiciones básicas para atender este tipo de solicitudes y se establecen los mecanismos para que su atención sea pronta y expedita, a efecto de que las áreas responsables de conocer este tipo de solicitudes contaran con los elementos necesarios para hacerlo.

2.- La protección de datos personales en poder de la Comisión Nacional de Derechos Humanos.

Con el objeto de informar sobre las políticas de la Comisión Nacional de Derechos Humanos en relación con la protección de datos personales, el 30 de septiembre de 2003 el Consejo Consultivo de la misma emitió el acuerdo 7/2003 en el cual se establece que las personas que entreguen información y datos personales a la Comisión, se les comunicará que la información que ellos proporcionen podrá ser suministrada a un tercero que lo solicite, después de un lapso de 12 años, contados a partir de la fecha en que se resuelva el asunto respectivo.

En el caso de que se acrediten violaciones graves a los derechos humanos se podrá tener acceso al expediente desde el momento en que el mismo sea concluido, de acuerdo con lo

dispuesto por el artículo 14 de la Ley Federal de Transparencia y 10 del Reglamento de dicha ley para la Comisión Nacional de los Derechos Humanos.

Los datos personales que esta Comisión reciba serán manejados con fines exclusivamente de identificación y se les dará un tratamiento confidencial, esa es la prevención, la leyenda que a toda persona que se acerca a la Comisión Nacional a solicitar su intervención se le es entrega.

Por otra parte, la Comisión Nacional de Derechos Humanos, desde el año de 1990 se ha ocupado de la seguridad de la información contenida en los distintos sistemas que conforman sus bases de datos, la clave incluye datos personales de los quejosos, agraviados, incluso, de presuntos responsables o responsables de las violaciones a derechos humanos.

En ese sentido, se mantienen permanentemente actualizadas las medidas de seguridad para controlar el acceso a la base de datos de la comisión, el cual está restringido a las estaciones ubicadas en las distintas instalaciones con que cuenta la institución a efecto de evitar el acceso a través de sistemas remotos, lo cual contribuye a elevar los niveles de seguridad.

Aunado a lo anterior, el acceso a la base de datos está limitado a un determinado número de funcionarios, quienes en su mayoría lo hacen en la modalidad de consulta, mientras que los responsables de ingresar información o bien realizar modificaciones en caso de que sea necesario están plenamente identificados.

La experiencia de la Comisión Nacional en relación a solicitudes de acceso y corrección de datos personales.

En el período comprendido entre el 12 de junio de 2003 al 31 de octubre del presente año, ante CNDH se han presentado tres solicitudes en materia de corrección de datos personales, mismas que fueron presentadas en el mes de enero, en las cuales se solicitaba la modificación de datos personales de solicitantes de acceso a la información, situación que fue realizada de conformidad a las peticiones.

Desde el momento mismo en que empezaron a atenderse y a resolverse las solicitudes de acceso a la información, de acuerdo con lo dispuesto en la Ley Federal de Transparencia, se dio acceso a éstas a través de su consulta en la página de Internet de la institución, en la dirección www.cndh.org.mx, pueden consultar cada una de las solicitudes que han sido presentadas y las respuestas que se da a las mismas, claro, eliminando aquellos datos personales.

4.- La protección de los datos personales frente al acceso a la información.

El artículo Cuarto de la Ley de la Comisión Nacional de los Derechos Humanos establece que el personal de la misma deberá de manejar de manera confidencial la información o documentación relativa a los asuntos de su competencia.

Lo anterior no ha impedido al Ombudsman nacional, tal como se ha dado cuenta anteriormente, dar cabal cumplimiento a las disposiciones de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

En ese sentido, es importante resaltar que durante el período comprendido del 12 de junio del 2003 al 31 de octubre de 2005, únicamente el 6.85 de las 321 solicitudes presentadas han sido consideradas como reservadas, porque así lo dispone tanto la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, como el Reglamento de ésta para la Comisión Nacional de Derechos Humanos.

A mayor abundamiento, en este período sólo se han presentado trece recursos de revisión en contra de la respuesta entregada al solicitante o con motivo de la resolución del Comité de Información de la Comisión Nacional. De este universo, dos se encuentran en trámite,

mientras que las once restantes han sido concluidas.

No obstante lo anterior, existe la preocupación de que aún y cuando en las solicitudes de acceso a la información se otorgue acceso a las mismas eliminando los datos personales, en algunos casos esto no es suficiente, ya que al interrelacionarla sea posible inferir la identidad o demás datos personales de los quejosos y/o agraviados.

Para quienes han depositado la confianza en el Ombudsman nacional con la finalidad de buscar protección en contra de los abusos de autoridad, lo menos que desearían es que un tercero, la contraparte en algún procedimiento o, inclusive, las mismas autoridades responsables de la violación a sus derechos fundamentales tuvieran acceso a los asuntos por ellos planteados ante la Comisión.

Por desgracia tal afirmación cobra fuerza al recordar algunos casos en que los quejosos y/o agraviados ante las Comisiones de Derechos Humanos en nuestro país, han sido objeto de amenazas, intimidaciones e incluso la muerte al denunciar acciones u omisiones de las autoridades, como es el lamentable fallecimiento del señor Rodolfo Benítez Figueroa, tal como se recuenta en el texto de la recomendación nueve de 2001, misma que puede ser consultada en el sitio de la Comisión Nacional.

A manera de conclusión, a partir de este ejemplo surge la necesidad de reflexionar sobre el hecho de que el garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales trasciende el propósito de asegurar su adecuado tratamiento e impedir la transmisión ilícita y lesiva para la dignidad de derechos del afectado, en algunos casos obedece más a la imperiosa necesidad de garantizar la salvaguarda de su integridad e incluso el derecho a la vida, condición esencial para el desarrollo de la persona.

Esta situación en ningún momento debe utilizarse a manera de justificación, para que los sujetos obligados clasifiquen como reservada o confidencial la información en su poder, bajo un falso argumento de que toda la información pone en riesgo la vida o seguridad de determinadas personas.

Por ello, es urgente ampliar aquellas disposiciones normativas o inclusive crear una nueva legislación, a fin de que se reconozca la importancia de garantizar a los individuos su derecho a la autodeterminación informativa, sin afectar el derecho a la información de terceros.

Por ultimo, agradezco al Instituto Federal de Acceso a la Información Publica y a la Red Iberoamericana de Protección de Datos, la invitación a participar en este magnífico evento que ha permitido intercambiar experiencias y ampliar el debate en estos apasionantes temas, que son la Protección de Datos Personales y el Acceso a la Información, conceptos que se encuentran estrechamente entrelazados e inclusive, como se ha comentado, en algunas ocasiones parecieran entrar en conflicto.

Moderador: Alonso Gómez Robledo Verduzco. Comisionado del IFAI.

Pasaríamos ahora a la participación de Oscar Puchinelli. Doctor en Derecho por la Facultad de Derecho de la Universidad Nacional de Buenos Aires. Es profesor adjunto de Derecho Constitucional Uno y Derecho Constitucional Dos. Esta cátedra la imparte en la Facultad de Derecho de la Universidad Nacional de Rosario. Es Profesor a Cargo de Cátedra, Derecho Procesal Derecho Procesal Constitucional y Transnacional, en la Facultad de Derecho de la Universidad Nacional de Rosario.

Entre los premios obtenidos quisiéramos destacar el siguiente: El primer premio, Concurso Colegio de Abogados de Rosario, año 2003, en la categoría Derecho Público, con el trabajo *Los Desafíos del Hábeas Corpus* argentino, en el

centenario de la Constitución de 1853, a propósito del *Habeas Corpus* contra particulares y del *Habeas Corpus* colectivo.

Ponente: Oscar Puchinelli.

Muchísimas gracias, por la presentación, por la invitación del IFAI y de la Red Iberoamericana, es un alto honor para mí compartir la mesa y por supuesto este evento que es tan trascendente de no solamente para México, sino para Iberoamérica en general.

Me permito leer un pequeño trabajo que salió en el diario *La Tercera*, de Chile, el día 31 de octubre. Unos parrafitos, pido disculpas si alguna de las palabras no es muy apropiada. Es una publicación de Jaime Bayly, que es un periodista peruano bastante conocido, que llama trabalenguas. Y ahí dice, en un párrafo, que creo que es el menos dificultoso para mí mencionar, les dice: *Checa que viene la ley, dijo un mexicano; para que bien la cana chabón, dijo un argentino; ojo, huevón, ahí están los pacos, dijo un chileno; corre que vienen los maderos, dijo un español; suave que viene los tombos, dijo un peruano*.

Esto que de algún modo sirve como prolegómeno de lo que voy a decir, tiene que ver con la riqueza de la lengua española, que sinceramente no podemos dejar de destacar, y la riqueza que fue destacada también en la Declaración de Montreux, en cuanto a que el derecho a la protección de datos es un derecho universal, pero que debe respetar la diversidad.

En nuestra América Latina, desde luego hay una gran diversidad, y una gran diversidad de enfoques en materia de protección de datos, en materia de *Hábeas data* que llevan precisamente a una consecuencia negativa.

La consecuencia negativa precisamente es que la terminología utilizada, incluso los conceptos muchas veces son hasta contradictorios y conspiran precisamente con la finalidad que debe tener todo sistema de protección de datos, que es por supuesto que haya una claridad conceptual, que haya una claridad terminológica, y que por supuesto se simplifique al máximo todo lo que tiene que ver con su regulación, por supuesto no dejando de lado regulaciones fundamentales.

En este punto quiero hacer algunas aclaraciones, esta mesa se refiere precisamente al control que ejercen los gobiernos, y en esto yo me voy a detener un poquito en analizar algunas de las formas de control o las que debieran estar y cómo han sido evaluadas en líneas generales en derecho comparado. Los medios de protección pueden ser legislativos administrativos o judiciales; y aquí tenemos múltiples variantes, tanto en América Latina, como en Europa, que sin embargo está bastante homogeneizado a partir de las normativas internacionales.

Los medios de protección legislativos o de índole normativo general, podríamos decirlo, parten de tres fuentes fundamentales. La primera son los convenios, digamos, en orden ascendente, descendente, los convenios regionales. En América Latina, desde luego, no tenemos todavía una convención americana, aunque hay proyectos en la OEA al respecto y de algún modo los trabajos de la Red están tendiendo a esta concreción.

Luego vienen las constituciones que en el caso de América Latina a partir de las reformas del regreso generalizado de la democracia en la década de los ochenta hizo lo que podía ser, crear lo que se llamó el *Hábeas data* con distintos matices en cada uno de los países, porque lo que hizo fue crear una acción de garantía prácticamente sin desarrollar el derecho al cual debía proteger.

Este es uno de los motivos por los cuales hay una gran diversidad, no solamente en terminológicas en las legislaciones y conceptual, también, si no en los diversos proyectos que hoy están en los parlamentos de los distintos países latinoamericanos que todavía no tienen ley de protección de datos.

Destaco y rescato la figura del *Hábeas data* porque de algún modo ha sido puesto en cuestionamiento. Aquí en México ustedes tienen un amparo que es gigantesco, en América Latina hay mayor diversificación de institutos de garantía de acciones procesales constitucionales y una de ellas es precisamente el *Hábeas data* que en realidad se limita a eso pero tiene una gran utilidad.

Creo y en esto estoy parcialmente en desacuerdo con lo que el profesor Chirino Sánchez, no es una acción que sólo llegue cuando no haya nada más nada que hacer, precisamente uno de los roles que fundamentalmente ha tenido América Latina, ha sido el rol preventivo.

Desde luego muchas de las veces también llegan cuando los daños están siendo ocasionados. Pero en materia de protección de datos, salvo que se trate de la desaparición física de una persona o la lesión a la integridad corporal, siempre se está a tiempo de prevenir daños posteriores, es decir que el *Hábeas data* siempre sirve, salvo esas situaciones donde no se puede ejercer.

Dentro de los medios de protección están desde luego las leyes de protección de datos y otras normas que no son leyes generales de protección de datos, pero que desde luego contribuyen a esa protección.

En este punto, ayer se relataba con mucho detalle las diferentes leyes que hay en México, incluyendo el Código Civil, el Código Penal Federal, la Ley Federal Financiera, la Ley de Instituciones de Crédito, la Ley Federal de Protección al Consumidor, la Ley de Información Estadística y Geográfica, la Ley de Responsabilidades del Funcionario Público, la Ley de Transparencia y Acceso a la Información Pública, todas ellas tienen algo que ver con la protección de datos.

Y en este punto, que voy a evaluar después, desde luego que es bueno que las autoridades relativas a cada sector, incluso las autoridades electorales también tengan función en este aspecto, tengan y cuiden los datos personales.

Pero también sí es muy importante que haya una autoridad única que de algún modo establezca criterios uniformes, porque si la legislación no es clara se puede producir una serie de discordancias en el ordenamiento interno que no es aconsejable, por lo menos de frente a lo que se le debe proporcionar a los ciudadanos.

También en la protección judicial ya hablábamos de la *Hábeas data*, pero también a través de sanciones penales, a través de sanciones civiles, un medio eficaz de control a falta de la ley de protección de datos han sido los reclamos indemnizatorios.

Muchos tratantes de datos han debido adecuar sus prácticas precisamente porque los jueces han sido sumamente rigurosos en la aplicación de sanciones de carácter civil frente a los tratamientos abusivos de los datos.

Las sanciones civiles, desde luego están propiciadas desde el orden internacional, el principio octavo de las directrices de la ONU, el artículo 23 de la directiva europea 95 46, un documento del año 2004 del Grupo del artículo 29 de la Unión Europea, el artículo 23 de la ley chilena, el artículo 19 de la ley española, en fin. La mayoría de las legislaciones aluden al deber de indemnización. Los jueces han sido sumamente estrictos en cuanto a la apreciación del daño y, sobre todo la reparación del daño moral e independientemente del daño material sufrido por quienes fueron objeto de tratamientos indebidos de datos personales.

Y desde luego las sanciones penales, ahí hay una discusión si deben o no estar dentro de una ley de protección de datos. En el caso español se prefiere estar fuera de la ley de protección y, en el caso argentino se optó por algo diferente, se incorporó en la ley de protección de datos, pero como una incorporación anexa al código penal.

En el campo de la protección administrativa, el deber de protección a través de una autoridad de control independiente surge claramente de la directiva 95 46 de la declaración Montreux que decíamos antes y de la resolución 45 95 de la ONU, el principio rector número ocho.

Es decir, que esto de que haya una autoridad independiente es y diría yo, única, por lo menos en cuanto al nivel último de decisión, si bien debe haber otras autoridades que puedan aplicar y que deben aplicar los principios de la protección de datos esto ha traído determinadas formas de regulación, desde luego, en el derecho comparado tenemos muchas, el Privacy Commissioner of Canadá, el Garante per la protezione dei dati personali en Italia, la Agencia Española de Protección de Datos, que es una autoridad independiente, en el caso argentino la Dirección Nacional de Protección de Datos que depende del Ministerio de Justicia, en la ley chilena el Servicio del Registro Civil de Identificación, en la ley uruguaya una comisión que depende del Ministerio Económico y Finanzas, en México vemos una diversificación, pero también lo elabora el IFAI, es muy importante y también desde luego la derivada del control de la ley de defensa al consumidor, es decir, hay diversas formas de controlar, algunas son de fracción parlamentaria, otras son de extracción ejecutiva, otras son autoridades independientes.

En este punto, me parece importante destacar que la independencia central en cualquier sistema de protección, por ahí una dependencia, la defensoría del pueblo puede ser una alternativa.

Desde luego, normalmente, porque en este caso hay muchas diferencias regulatorias en los distintos países, normalmente el defensor del pueblo actúa sólo sobre la actividad de la administración y obviamente esto es poco, porque el tratamiento de datos no solamente en la administración pública en el sentido del Poder Ejecutivo, sino también lo hace el propio Legislativo, lo hace el Poder Judicial y lo hacen los particulares, con lo cual pareciera más conveniente que fuera de tipo independiente y no de extracción parlamentaria ni de extracción ejecutiva.

En el caso de Argentina una de las observaciones a la declaración de país con nivel adecuado de protección por parte del grupo de trabajo, artículo 29 de la Directiva Europea, ha sido que desde el punto de vista normativo no existe independencia en el órgano de control y tampoco hay legislación en los Estados federados que de algún modo esté de acuerdo con éste y con la legislación federal.

Esto, sin embargo, no ha sido óbice para el enorme despliegue que ha hecho el Director Nacional de Protección de Datos, quise poner en el currículum a último momento, porque para mí es honor, aunque sea un dato aparentemente negativo, haber perdido el concurso con el doctor Travieso, que está haciendo una gran labor desde que asumió la dirección de la Dirección Nacional.

Y desde luego también ser honesto en decir que me gustaría que fuera formalmente más independiente, aunque lo sea desde el punto de vista personal, ¿no? Me gustaría que realmente podamos lograr una Dirección Nacional que no sea un apéndice desde el punto de vista formal del Ejecutivo, sino una Dirección Nacional que sea un órgano extra-poder en todo caso y no una mera dependencia.

En este punto, ya no me va quedando mucho tiempo, quiero retomar un poquito lo que venía diciendo al principio, esto de provocarlos con las cuestiones terminológicas.

Nosotros en la primera sesión hablábamos de varias cuestiones relativas al derecho fundamental a la protección de datos y surgieron al lado de las mesas algunas contradicciones con esa posición, contradicciones que surgen de las distintas posiciones o las distintas culturas jurídicas que hoy se están volcando en este foro.

Yo insisto en la necesidad de unificar criterios y en esto insto a la Red de la cual formo parte en hacer esfuerzos para que en las legislaciones nacionales unifiquen las terminologías.

Me parece que utilizar la palabra derecho a la protección de datos es el término adecuado, me parece que es superador de otras construcciones anteriores, por ejemplo, libertad de informática, incluso, intimidad informática, *Hábeas data* que se usaba como derecho, incluso hoy se usa como sinónimo de derecho, que en realidad no lo es, el *Hábeas data* es una garantía de otros derechos y me parece que esto es muy importante que se pueda visualizar desde el punto de vista conceptual.

Por ejemplo, en los proyectos de Colombia, incluso, en la doctrina de la Corte Constitucional se usa la palabra derecho de *Hábeas data* como la primera frase que tiene que ver con el acceso y después a la segunda fase se llama derechos conexos de rectificación, etc.

Me parece que tendríamos que tratar de unificar y rescatar el sentido inicial del *Hábeas data* que fue una acción procesal constitucional que nació en una constitución brasileña del ochenta y ocho y que tenía como finalidad actuar sobre los datos personales para tutelar, en ese caso se pensó mucho en la libertad física, en la integridad física, en el derecho a la vida, porque se trataba de la idea de los constituyentes a acceder a los bancos de datos oficiales para prevenir futuras discriminaciones, en función de que está volviendo la democracia en los bancos de datos de la dictadura.

Entonces, volver a esa idea de la *Hábeas data* como un mecanismo protector, limitado a eso y no confundirlo conceptualmente, y por supuesto el derecho a la protección de datos sería superador también, en mi opinión, del concepto de autodeterminación informativa, que fue acuñado por el Tribunal Federal alemán, en 1983, en la Famosa Ley de Censo de la Población, que si bien coincido con el profesor Chirino Sánchez, no debemos hacer una cuestión determinológica muy aguda, sí digo que su propia denominación apunta prácticamente a uno sólo de los aspectos, que es la facultad de, uno, de autodeterminar o de decidir qué se hace y qué se no se hace con sus datos, y en realidad esto es mucho más que eso.

Me parece que conceptualmente la palabra queda superada. Les doy solamente un ejemplo que me viene a la memoria en este momento: En Argentina sobre protección de datos es un caso llamado Urteaga, que es el caso del hermano, un desaparecido, que solicita información sobre los restos de su humano y la Corte dijo, de manera clara, que a través de la *Hábeas data* se podrían garantizar muchos derechos, entre ellos la identidad, la dignidad, la intimidad, el honor, la libertad, la propiedad e incluso, y en esto me detengo, el derecho al duelo y el derecho a enterrar a los difuntos.

Y ustedes dirán: ¿Qué conexión puede tener con la protección de datos? Bueno, precisamente este es uno de los puntos interesantes.

Desde luego esta persona reclamaba el derecho de acceso a los datos personales de su hermano desaparecido.

También propongo que además de llamar derecho a la protección de datos, a este nuevo derecho, como lo hace el artículo 8 de la Carta de Derechos fundamentales de Niza de 2000, se hable de una nueva disciplina que es el derecho de la protección de datos.

Es una disciplina claramente interdisciplinaria, que está muy conectada obviamente con el derecho a la información, que fantásticamente creo, aquí se ha visto como dos caras de una misma moneda, como también decía el profesor Chirino Sánchez, en la regulación de la ley y las facultades que se le da al IFAI.

El acceso a información pública y la protección de los datos personales, no pueden estar desvinculados y es bueno que haya un solo criterio en estos dos puntos.

Las causales para no permitir el acceso a la información pública y las causales para denegar la protección de los datos personales son las mismas: Seguridad nacional, seguridad pública, defensa de intereses de terceros, salud pública, etc. Allí es bueno que haya un criterio rector uniforme.

Desde luego, todo está en el ámbito del derecho a la información, como gran madre de esta disciplina. Ya quedan superados, desde luego, los conceptos, que lo ligaban al derecho informático o a la informática jurídica. Éstos al principio eran quienes habían tratado, los especialistas en derechos informáticos e informática jurídica, los que habían tratado esta temática.

Con esto voy a ir terminando y simplemente para mostrarles algunas de las diferencias que tenemos en las distintas legislaciones y que ameritaría unificarse.

Les digo que, por ejemplo para la ley chilena, lo que nosotros debiéramos denominar sistemas de información en general, es denominado como registro de banco de datos, en la legislación española como ficheros, en la Argentina como archivo, registro, base o banco de datos, en la legislación peruana como banco de datos, en la legislación uruguaya como archivo, registros, bases, con relación a quienes tratan los datos, en Chile se les trata como responsables, en España se distingue entre responsables de fichero y de tratamiento, en Argentina se divide entre responsables de la base de banco de datos y usuario, pero usuario utilizado de una manera diferente a la que se utiliza en el resto de la legislación, se utiliza en el sentido de responsable de tratamiento; también en España se alude a encargado de tratamiento, esa normativa no tiene un reflejo exacto en el resto de las legislaciones.

Cuando se alude al titular de los datos se alude de manera diferente, como titular de los datos, como afectado o como interesado, como concernido, etc., no hay uniformidad en la denominación. Esto se debe precisamente, en algunos casos, a la riqueza de la lengua española y en algunos otros se debe a errores conceptuales que no tengo en este momento forma de desarrollar.

En este punto quisiera dejar como mensaje la necesidad de unificar, a fin de que, en definitiva, la legislación se aclare en uniforme.

Rescato lo que decía el doctor Travieso al principio, cuando se puede copiar es bueno copiar. En este punto yo creo que si las legislaciones fueran exactamente iguales, por lo menos en lo sustancial y en lo conceptual estaríamos en una perspectiva de protección mucho más eficiente, mucho más eficaz.

Y desde luego esto es muy importante para que no se vea en la práctica de algún modo cumplido aquel exorcismo literario que George Orwell de alguna manera hizo a través de *1984*, y que la ley en definitiva no sea una telaraña que detenga los insectos y deje pasar a los pájaros.

Moderador: Alonso Gómez Robledo Verduzco. Comisionado del IFAI.

Se abrirá en espacio para las preguntas y respuestas.

Al licenciado Carlos Arce Macías. ¿Existe una propuesta de Ley de la PROFECO sobre la protección de datos personales en asuntos comerciales y electorales? Si la respuesta es afirmativa, ¿en qué consiste?, negativa, ¿entonces por qué?

Ponente: Carlos Arce Macías.

Rápidamente, no. No tenemos esta atribución como para hacer una iniciativa ni mucho menos. No hay propuesta al respecto de parte de la PROFECO.

La PROFECO simplemente tiene una serie de funciones de protección de datos personales. Como ya lo comenté, las listas de no llamadas, que es una cuestión facultativa, podemos hacerlo o no y depende sobre todo de presupuesto. Esperamos que en el presupuesto

2006 poder llevar a cabo precisamente este sistema de inscripción de listas para no ser molestados vía telefónica en su domicilio.

Por otra parte, conozco simplemente la iniciativa que existe en el Congreso. En el Congreso está aprobado por el Senado ya una iniciativa. Está en minuta en la Cámara de Diputados, tiene que ser discutida y que ya fue aprobada previamente, por supuesto en el Senado.

Sin embargo, reitero, primero, la secuencia lógica en cuestión de datos personales debería de haber sido, primero: Ley de archivos, Ley de Protección de Datos Personales y la Ley Federal de Acceso a la Información Pública Gubernamental.

Al inicio de este sexenio se vio que las posibilidades estratégicas dentro del Congreso, y creo que así fue el asunto, se daba en la posibilidad de tramitar la Ley Federal de Acceso a la Información Pública Gubernamental, la cual pudo salir a inicios del sexenio y ahora esta ley precisamente esta siendo el efecto contrario, o sea, percutiendo la necesidad de la Ley de Datos Personales y por supuesto de la Ley de Archivos, porque el otro asunto a donde vamos a llegar es dónde están nuestros datos, quién protege nuestros datos, quién utiliza y cómo se guardan y resguardan nuestros datos que sería la Ley de Archivos.

De tal manera que el asunto que como yo ya lo comentaba está cojo mientras no tengamos la Ley de Protección de Datos Personales y la otra muy importante, Ley de Archivos.

Por lo pronto no hay ni habrá ninguna propuesta por parte de PROFECO, hay minuta en la Cámara de Diputados en este momento.

Moderador: Alonso Gómez Robledo Verduzco. Comisionado del IFAI.

Procurador le pediríamos que pueda seguir con el micrófono porque es otra pregunta que se le formula.

¿Cómo sancionar a las empresas y al mismo gobierno cuando éste último vende los datos a particulares?

Ponente: Carlos Arce Macías.

Bueno, evidentemente en el gobierno sí habría, dependiendo de la diferente legislación, habría responsabilidad de los servidores públicos a nivel individual y podrían ser sancionados, por supuesto, ya ha habido algunos casos en el IFE por ejemplo, pero ahí hay ciertos controles y la Ley Federal de Acceso a la Información Pública Gubernamental previene también una parte de datos, de protección de datos personales y se previno así precisamente en el conocimiento de que no había una ley ex profeso para la materia, igual que hay una serie de instrucciones en relación a archivos.

En estos momentos en relación a las empresas comerciales, pues evidentemente no se puede hacer nada, no hay ningún tipo de regulación al respecto y hay una negociación continua entre ellas para recabar listados de datos personales, incluso en el Internet se pueden encontrar por ahí la venta de discos de grandes ficheros, grandes listas de datos personales de ejecutivos, de personas de ciertas condiciones económicas, etcétera.

No hay ningún tipo de regulación que acote en estos momentos esa situación, cosa que ya se ha comentado aquí, es uno de los problemas graves que estamos enfrentando y los problemas tecnológicos incluso.

Doy un dato. Incluso con cierto Software apropiado podría haber un seguimiento por llamadas telefónicas de dónde se mueve la gente. Aparte de la situación relativa al ADN por ejemplo, que podríamos saber prácticamente de qué nos vamos a morir y de qué nos vamos a enfermar, y para las empresas puede ser muy importante esto no solamente para las médicas, las de seguros, etcétera.

Podemos también saber dónde está la gente, en qué zonas se mueve, en qué zonas comerciales.

Podemos tener un seguimiento con la minería de datos, como comentan, podríamos tener un conocimiento muy preciso de todo el comportamiento comercial de una persona para saber qué le vendemos, cómo le vendemos, qué mercadotecnia usamos, en qué áreas se desplaza, etcétera.

Este es el problema. Estas son las agendas del siglo XXI, es lo que se tiene que estar discutiendo en México porque es lo que se está discutiendo en el mundo y no estar atorados en otros tipos de agendas que tenemos que resolver rápidamente.

Moderador: Alonso Gómez Robledo Verduzco. Comisionado del IFAI.
Pregunta para el Consejero Andrés Albo Márquez: La información que mencionó respecto de las aportaciones de militantes y/o simpatizantes de los partidos ¿ya está cargada o a la vista en la página Web del IFE?

¿Cuál fue la sanción que se le aplicó al servidor público que divulgó información relativa a datos personales, del caso que se presentó en el IFE? Según mencionó usted en su exposición.

¿Qué medidas como resultado de esta experiencia se aplicaron o se aplicarán?

Se ha planteado en México la implementación del voto electrónico. ¿En este caso un sistema de voto electrónico debería implementar medidas para evitar que se identifiquen las preferencias políticas de los electores? ¿Hay un marco normativo que permita evitar esa situación?

Ponente: Andrés Albo Márquez.

En lo relativo a las aportaciones sí hay un acuerdo que desde el 2003 hace pública las aportaciones, si no mal recuerdo, las aportaciones de los militantes y de los simpatizantes de los partidos políticos y éstas ya se encuentran en Internet.

Los nuevos sistemas que se están instrumentando para recabar fondos o por la vía de las tarjetas de crédito o por las vías de aportaciones directas vía telefónica, estos todavía no se echan a andar, todavía no tenemos reportes, todavía no se ha fiscalizado, pero desde luego va a ser objeto de publicación.

En el caso de las aportaciones vía telefónicas se solicita al aportante algunos dato que permiten el consentimiento del aportante o cuando menos del propietario de la línea.

El funcionario de nivel administrativo que fue objeto de la investigación y, bueno, se le demostraron algunas responsabilidades en el caso este tan penoso de utilización de bancos de datos, bueno, ahora está en la cárcel.

A partir de ello sí el Instituto ha realizado varias acciones, algunas de carácter práctico, inmediatas, de carácter tecnológico como reforzar los sistemas de información, acceso, control, de estos datos, incluso desde modificaciones en la infraestructura material y de resguardo de esta información.

Pero también ha habido acciones de tipo reglamentario, de tipo normativo en los alcances que tiene el Instituto, que básicamente ha sido, pues, reflejar en el Reglamento de Transparencia una parte específica para todos estos datos. Pero dada las particularidades del padrón también ha habido algunos acuerdos al respecto.

Pero diría que además de estos sistemas se tiene previsto un sistema tecnológico de control mucho más preciso.

En el caso del voto electrónico, bueno, ya el mismo voto que se realiza en urnas tiene una reglamentación muy precisa y muy estricta en términos de la confidencialidad, los candados que le llamamos coloquialmente para impedir toda identidad del votante. A pesar de ello, bueno, en cumplimiento de ello sí se hacen algunos estudios, incluso, recientemente se publicaron los primeros datos de preferencias políticas a

nivel agregado, votos, algunas características en una muestra de urnas.

En el caso del voto electrónico que nosotros no estamos contemplando este instrumento para las próximas elecciones, sino que tendría que ser de manera experimental hasta probablemente el 2006, lo que se está buscando es desarrollar una tecnología propia, pero también se está viendo cuáles son las ventajas del voto electrónico en algunos estados, incluso en algunas partes del mundo, pero uno de los requisitos y de los elementos que se están tomando en consideración justamente es la confidencialidad de los votantes y de los momentos en los que se ejerza el voto.

Moderador: Alonso Gómez Robledo Verduzco.

Para el doctor Alfredo Chirino Sánchez. Ya que no pudo exponer toda su ponencia, no sé si entendí su idea. En México la privacidad del derecho de autodeterminación de la información ha sido del Estado y no de los particulares.

El artículo Octavo de la Constitución garantiza, desde hace años, que un funcionario debe responder a la petición de un ciudadano. Pero no daba el derecho a que le informara de la actividad de dicho funcionario, como ahora.

Hasta donde entendí de su exposición, la privacidad se refiere a que en América Latina se considera que sólo el que tiene algo que ocultar, es el que pide precisamente esta privacidad, no acceso a sus datos personales; quién no tiene nada que ocultar, obviamente, entonces lo deja precisamente a plena libertad.

Y en este caso yo considero, es mi experiencia, que en el gobierno mexicano eso es lo que se ha dado. La privacidad era exclusivamente por parte del Estado y cada vez que se pedía información, antes de la Ley de Transparencia, simplemente se trataba como si fuera una cuestión de seguridad nacional, cuestiones muy sencillas, cuestiones bastante puntuales acerca del funcionamiento del Estado.

Entonces, yo quisiera que el doctor me aclarara, si es que entendí mal su exposición, a qué se refería con esto.

Ponente: Alfredo Chirino Márquez.

Mucha gracias por la pregunta, yo la verdad había quedado con muchos deseos de contestarle al doctor Puchinelli, al cual me da mucho gusto conocerlo, ya que había leído su libro sobre la situación del derecho de *Hábeas data* en el sistema Indoamericano, y me parece un excelente libro.

Voy aprovechar entonces para contestar la pregunta que me hacen, y decir algo que está relacionado con los criterios terminológicos a los que aludía mi colega argentino.

Me parece que yo quería hacer alusión a la diferencia que hay entre el tratamiento jurídico o dogmático del derecho a la privacidad, a la intimidad y a la autodeterminación informativa y su correlato cultural.

Me parece, y aquí estoy hablando únicamente de la cultura social de mi país, la cultura de la privacidad o de mantener asuntos en la intimidad siempre refleja el sentimiento social de sospecha, de que aquel que oculta algo es porque efectivamente quiero esconder algo de la vista pública.

Esa es la situación cultural de mi país, que es intransferible a otros países, y sólo puedo hablar de ella, porque es la que conozco bien.

Lo que usted me plantea de México a partir de la evolución constitucional del derecho de petición y respuesta, que está consignado en casi todas las constituciones liberales posteriores a la Segunda Guerra Mundial refleja efectivamente que el derecho de acceso a la información era puramente formalista, se refería exclusivamente a tener acceso a registros y archivos públicos, y muchas veces se ridiculizó ese derecho diciendo para lograr mejor acceso a los archivos públicos lo que hay que hacer los aparcamientos más grandes.

El derecho al acceso a la información pública quedó ridiculizado mucho tiempo, considerado exclusivamente como un derecho constitucional de petición.

Con los avances que se han dado en la discusión sobre el acceso de la información, repito, principalmente en temas de acceso a la información pública en materia de protección ambiental, es que hoy, efectivamente, el derecho de acceso a la información es la contracara, el anverso de la moneda relacionada con el derecho de la protección de datos.

Que ocurra eso en México en relación con los funcionarios públicos, y que por mucho tiempo esa situación de secrecía, como dicen ustedes, se refiere específicamente a la vida privada y a las gestiones privadas, que de alguna manera están conectadas con lo público del ciudadano, probablemente tiene que ver con una nueva atmósfera democrática que se vive no sólo en México, sino en toda América Latina.

Aprovecho la pregunta solamente para decir al doctor Puchinelli, que en efecto mi ataque al tema del *Hábeas data* es para generar ese debate que no hemos podido generar y que tal vez sería muy interesante tener, y era precisamente para causar esa sensación de que el con el *Hábeas data* realmente estamos solamente en una parte de la discusión.

Pero yo tengo que reconocer públicamente que sin *Hábeas data* no tendríamos la evolución jurisprudencial que se ha dado en mi país, hasta el punto de reconocer a través de una garantía procesal el derecho sustantivo a la protección de datos.

Por esa razón creo que, en efecto, hay que discutir esto desde un punto de vista dogmático, normativo, pero no podemos perder la vista del bosque por un solo árbol.

Lo comentaba ahora con la doctora Sepúlveda Toro, es indudable que la mesa está sobre los temas del gobierno y los datos que maneja, y discutir sobre las múltiples formas de observar este derecho y esta garantía moderna en las sociedades de la información, podría hacernos perder la oportunidad histórica y política de alcanzar el derecho a la protección de datos que parece ser la única garantía en una sociedad de información, donde hasta el dinero ha perdido su valor, y la información tiene el más importante desde que aquel importante filósofo dijo: El poder la información lo es todo.

Moderador: Alonso Gómez Robledo Verduzco. Comisionado del IFAI.

Pediría ahora la respuesta a Andrés Calero Aguilar.

Ponente: Andrés Calero Aguilar.

Es un planteamiento que me voy a permitir leer para el entendimiento de la respuesta. Señala que la Academia Mexicana de Derechos Humanos solicitó información acerca del Consejo Consultivo de la CNDH y ésta pretextando que es confidencial la negó. La opacidad de la CNDH ha provocado la necesidad de un programa como Atalaya del ITAM para analizar y evaluar realmente la Comisión.

Dos cosas: El planteamiento es equivocado; las actas del Consejo Consultivo en su versión pública han sido entregadas a la Academia, el Consejo está integrada por personas que no son servidores público, por los cuales no se les puede obligar entregar la información y por lo tanto se hizo una versión pública.

Segundo. No sólo el programa Atalaya ha supervisado, analizado y estudiado la Comisión; existen programas de la Academia Mexicana de Derechos Humanos de FUNDAR, y de la Universidad de San Diego, a los cuales la Comisión ve con muy buenos ojos, estamos como organismo público autónomo sujetos a la disposiciones de la ley y, tal como se señaló anteriormente únicamente siete por ciento de las más de 300 solicitudes de transparencia han sido clasificadas porque así lo dispone la ley, como información reservada, únicamente menos del siete por ciento.

Moderador: Alonso Gómez Robledo Verduzco. Comisionado del IFAI.

Rápidamente dos últimas preguntas por obvio del tiempo.

A la doctora María Alejandra Sepúlveda Toro. ¿Qué experiencia tienen en Chile respecto a la aplicación de la ley de protección en los aspectos: financieros, información crediticia, acceso a la información, bancos de datos en gobierno *versus* protección de datos personales?

Ponente: María Alejandra Sepúlveda Toro.

La experiencia que tenemos respecto de el tratamiento de datos personales por los organismos privados se vincula principalmente respecto a reclamaciones que se realizan en torno a entrega de información, sin que esté pendiente la decisión o la definición de un nuevo crédito, solamente para la información general que podría tener un banco sin que necesariamente el titular de los datos esté haciendo unas gestiones específica de obtención de algún nuevo préstamo.

Por otra parte, la otra reclamación tiene que ver con mantener la información más allá de los plazos que se ha previsto en la ley, que se vincula con los cinco años desde que la obligación se hizo exigible o una vez que ya está prescrita la acción penal o administrativa. Yo diría que en ese contexto están más bien planteadas las reclamaciones.

Ahora, también hay reclamaciones que se realizan al servicio nacional del consumidor, que tiene que ver con temas vinculados al gran flujo de correspondencia que llega, sin que las personas hayan entregado sus datos para tales efectos.

Moderador: Alonso Gómez Robledo Verduzco. Comisionado del IFAI.

Terminaríamos con una última pregunta formulada al doctor Oscar Puchinelli, consiste en lo siguiente: ¿Qué riesgos considera usted que existen si la autoridad garante de la protección de datos personales depende directamente del Poder Ejecutivo? Es decir, que no sea autónoma e independiente o de creación o dependencia parlamentaria.

Ponente: Oscar Puchinelli

En primer lugar es una cuestión inicial de credibilidad. Cuando uno le da la función de control a un órgano dependiente del que va a controlar, evidentemente la gente no tiene mucha confianza, de entrada.

Si usted le va a decir al Poder Ejecutivo que es el que maneja la mayor cantidad de base de datos que tenga una dependencia, que lo va a controlar, esto es de alguna manera bastante, desde el punto de vista de la gente, bastante poco confiable, aunque la institución resulte confiable, un primer argumento arranca desde la necesidad de que el controlador no esté en la misma órbita del controlado, este es un principio básico del sistema en contrapeso.

Hay una tendencia general en los ejecutivos a de alguna manera utilizar los datos, yo puedo dar dos ejemplos de mi país: recientemente hubo campañas electorales y mucha gente ha recibido llamadas telefónicas del Presidente de la República para pedir su apoyo en la votación, no hay elecciones presidenciales, sino hubo elecciones legislativas y mucha gente que ni siquiera estaba, no era público su dato, digamos, en el directorio telefónico, también recibió las llamadas, es decir, esto requiere de alguna manera cierta fuerza para controlar ese tipo de situaciones.

Desde luego, muchas o la mayoría pueden no ser reconocidas, pueden no ser vislumbrada por la autoridad de control, pero sí digo que muchas veces hay una tendencia por parte del Poder Ejecutivo de utilizar los datos personales contra la propia Ley de Protección de Datos, incluso otras autoridades no necesariamente del Poder Ejecutivo, de autoridades electorales, hubo una gran discusión hace muy poco tiempo donde se incluyó en el padrón electoral disponible a

cualquiera el dato de afiliación partidaria y esto genera una gran discusión.

Desde luego, los criterios de la autoridad de control yo los entiendo absolutamente independientes, porque conozco a la persona que lo dirige, pero tal vez no se ha vislumbrado de esta manera por la sociedad en general, ¿me explico? Es decir, en un primer momento yo diría la autoridad de control no tiene que tener que relación con los sujetos que va a controlar, debe ser completamente independiente.

En el campo del defensor del pueblo se aplica lo mismo, el defensor del pueblo, en general, en las legislaciones latinoamericanas y ese es el origen, digamos, institucional del ombudsman es el control de la administración pública. Está bien, va a controlar los bancos de datos del Poder Ejecutivo, pero ¿qué pasa con los otros bancos de datos? ¿Naturalmente es una institución apropiada para controlar los bancos de datos privados? Aparentemente no.

No quiere decir que no pueda hacerse, uno en ingeniería constitucional puede modelar con distinto resultados de acuerdo a la idiosincrasia de cada país, pero me parece que siempre hay que atender a una autoridad independiente.

Y les digo mi experiencia personal, una de las cosas que no coloqué ahí en el currículum fue que asesoro a legislador y que usualmente me han consultado legisladores entre distintos lugares de mi país.

Cuando quieren dictar una ley de adhesión a la Ley Nacional de Protección de Datos y crear una autoridad de control, siempre, como pauta, digamos ineludible, era: ¿Por qué no ponemos la autoridad de control en el Poder Ejecutivo? Siempre la idea es por qué poner la autoridad de control en el Poder Ejecutivo, porque normalmente es lo que menos daño puede causar al gobierno.

Esto sin perjuicio de que como en el caso argentino hay independencia en autoridad de control, hay estabilidad, de alguna manera está cubierto por lo menos por el período en el que está designada la autoridad de control, pero hay que dotarla siempre una fuerte independencia, en este punto para mí me parece central.

Lo que no quiere decir, como dije antes, que las dependencias del Poder Ejecutivo también ejerzan su control en función de sus competencias, esto también es cierto, pero la decisión final debiere estar, por lo menos el criterio definitivo desde el punto de vista administrativo, porque después están los correctivos judiciales desde luego, y en esta actividad los jueces ha sido muy valorada por supuesto en América Latina y sobre todo en Argentina, Colombia, donde han tenido un gran desarrollo, el criterio definitivo debiera estar por lo menos en una autoridad independiente que unifique además ese criterio para los ciudadanos que no pueden estar sujetos a distintos criterios que puedan tener el Poder Ejecutivo en función de sus distintas reparticiones.

Esa es mi visión del tema, pero no pretende ser una visión que descarte las otras alternativas, simplemente es lo que entiendo que favorecería una mejor protección de los datos de carácter personal.

Perspectiva del sector financiero y comercial en la protección de los datos: los datos de crédito y el marketing directo

Mesa 5

Moderadora: Isabel Davara Fernández de Marcos. Consultora especialista en Protección de datos personales.

Daré lectura del currículum de nuestro conferencista Rafael del Villar Alrich. Estudió la licenciatura en Economía en el ITAM y tiene Estudios de Derecho por la UNAM; es doctor en Economía por la Universidad de Pennsylvania. Es profesor asistente en el Departamento de Economía de la Universidad de Texas; fue Ministro para Asuntos Económicos, hasta el 1993 en la Embajada de México en París.

Fue director del Centro de Estudios de Competitividad y profesor de Economía del ITAM, junto a su equipo realizó estudios sobre la industria de seguros, la adopción de tecnología en diversos sectores, así como sobre inversión extranjera.

Fue Director General de Estudios Económicos de la Comisión Federal de Competencia. En 1994 elaboró el Anteproyecto de Ley Federal de Telecomunicaciones, que entró en vigor en junio del 1995.

Fue Director General de Política de Telecomunicaciones y Negociaciones Internacionales de la Secretaría de Comunicaciones y Transportes de 1995 a 1996, y elaboró el diseño de subastas del espectro radioeléctrico y el Anteproyecto de Reglamento de Interconexión.

Ha participado en la elaboración de diversas leyes: Ley de Concursos Mercantiles, Miscelánea de Garantías, Ley de Sociedades de Información Crediticia, Ley de Transparencia y Acceso a la Información Pública y Anteproyecto de Ley Federal de Protección de Datos Personales.

Conferencia Magistral: Rafael del Villar Alrich.

Se van a dar cuenta que tengo poco que decir del marketing director, aunque tengo un aspecto que sí voy a mencionar.

Y voy a hablar, más que de lo que quisiéramos ver en un futuro, voy a hablar de ciertos problemas o ciertas oportunidades que se observan con el tema de información crediticia.

La plática tiene tres partes. La primera describe el papel que tiene el mercado de información crediticia, para el eficiente funcionamiento del mercado de crédito y la importancia de desarrollar este mercado.

En la segunda parte se muestran los avances que se han hecho en México, en relación a la protección de la información crediticia. Y en la última parte se presentan algunos retos para el futuro.

Vamos de lleno a la primera parte, que es el mercado de información crediticia y el eficiente funcionamiento del mercado de crédito.

En México a principio de los años 90 se pusieron en marcha múltiples reformas en materia financiera, las cuales entre otros factores permitieron que se reactivara el crédito al sector privado, especialmente a los hogares. No obstante durante esa expansión crediticia la economía no contó con un adecuado de crédito sobre personas físicas.

Ello limitó las posibilidades de la banca para administrar los riesgos de su cartera crediticia, lo cual contribuyó al incremento en la cartera vencida y a agravar la crisis de 1995.

Desde los años 50 el Banco de México había venido administrando un registro, llamado Servicio Nacional de Información de Crédito Bancario, para créditos bancarios de montos superiores a aproximadamente 20 mil dólares.

Con la Ley de Agrupaciones Financieras de 1990 se previó la creación de un mercado privado de información crediticia, que incluyera todo tipo de créditos.

Las reglas para la constitución y operación de los primeros *burós* fueron emitidas a principio de 1995, originalmente se autorizaron tres *burós* para personas físicas. De los cuales uno salió del mercado en 1997, y otro en el año 2000.

En el presente año ha sido autorizado un *buró* de crédito adicional. Conviene hacer una pausa en este momento y hacer unas reflexiones del impacto que tiene el Servicio de Información Crediticias sobre la disponibilidad de crédito a los individuos, y sobre el eficiente desarrollo económico.

Los mercados de crédito casi siempre presentan un cierto grado de asimetría de información entre prestatarios y prestamistas.

Los prestatarios o sujetos de crédito tienen mejor información sobre su disposición o capacidad de pago que los oferentes de crédito.

Las ganancias para los oferentes dependen tanto del precio del crédito, es decir, la tasa de interés, como de la probabilidad de repago que generalmente no pueden observar. Invierten recursos para intentar determinar el nivel de riesgo de los sujetos. Éstos tienen el incentivo a cooperar con los oferentes, si su verdadero nivel de riesgo es bajo, pero tienden a ocultar información si ésta sugiere una elevada probabilidad de incumplimiento.

En un mundo en el que no se comparte información entre oferentes de crédito Stiglitz & Weiss demostraron hace ya un cuarto de siglo, que el problema de selección adversa reduce los beneficio del mercado de crédito para prestatarios y prestamistas.

Cuando los prestamistas no pueden distinguir entre buenos y malos sujetos de crédito, a todos los sujetos se les cobra una tasa de interés que refleja el promedio de riesgo del grupo en su conjunto.

Este precio es mayor que el que están dispuestos a pagar algunos sujetos de crédito de bajo riesgo, por lo que éstos deciden no contratar los créditos, lo que reduce la base de demandantes de crédito de bajo riesgo elevando aún más la tasa promedio que se cobra a los prestatarios que se quedan en el mercado.

El problema de selección adversa muestra con claridad porqué la existencia de más información hace que los mercados de crédito

funcionen mejor. La existencia de información sobre la experiencia crediticia de los distintos sujetos permite distinguir o separar a las personas de bajo riesgo de las de alto riesgo y ofrecerles crédito a menores tasas de interés evitando que abandonen el mercado.

Además de selección adversa, los mercados de crédito están sujetos al denominado riesgo moral. Es decir, el incentivo que tiene el prestatario a incumplir sus compromisos de pago una vez que se le ha otorgado el crédito. Ello, a menos que su incumplimiento tenga consecuencias como es el caso de que en el futuro sus nuevas solicitudes de crédito sean rechazadas o se le dificulte obtener un trabajo.

Una vez que las personas saben que su historial crediticio va a quedar registrado en bases de datos, tienden a evitar este tipo de comportamientos oportunistas.

Varios estudios, por ejemplo Pagano y Japelli en 1993 han mostrado cómo el compartimiento de la información puede reducir los problemas de selección adversa y riesgo moral e incrementar el volumen de crédito en beneficio del desarrollo económico.

Los incentivos de los oferentes de crédito a compartir información de deudores referente a su experiencia de pago, las obligaciones actuales y su nivel general de exposición, aumentan con el tamaño del mercado de crédito y el número de oferentes de crédito, la movilidad y la heterogeneidad de los deudores y con los avances y reducciones de costo de las tecnologías de información.

La intuición de estas afirmaciones es simple, a medida que aumenta el tamaño del mercado de crédito y el número de oferentes de crédito crece, la información sobre la experiencia de crédito de los sujetos está más fragmentada y por ende el compartimiento de información resulta más benéfico.

La movilidad y heterogeneidad de los deudores reduce la probabilidad de que un prestamista pueda fijar precios competitivos por los créditos que ofrece, basándose exclusivamente en su experiencia.

Otros oferentes que decidan compartir información tendrían una ventaja competitiva en el mercado de crédito. Los avances en las tecnologías de información y comunicación reducen los costos de formar y administrar bases de datos, es decir, los costos de los *Burós de Crédito*.

Sin embargo, también existe un incentivo que va en la dirección contraria, es decir, un incentivo a no compartir información entre oferentes. Este incentivo se ocasiona por el temor a la competencia por la entrada de oferentes adicionales y, en general, el temor por una competencia más intensa en el mercado. Ello, debido a que la información que permite distinguir a sujetos de crédito de alto y bajo riesgo es más accesible a los competidores.

Los *Burós de Crédito* o Sociedades de Información Crediticia son un tercer participante integral en los mercados de crédito. Son, no sólo un vehículo para agregar información de los oferentes y fungir como una especie de cámara de compensación de información crediticia, si no también un vehículo para disciplinar y sancionar aquellas instituciones que no les reportan correcta o cabalmente al poder excluirlos de sus servicios.

Si bien los oferentes tienen el incentivo a no compartir información de sus buenos deudores o incluso difundir información falsa sobre ellos, con el objeto de evitar que sus competidores los atraigan con mejores ofertas, los *Burós de Crédito* disciplinan a los oferentes en contra de estas acciones que perjudican a los mejores deudores. Para poder operar eficientemente y ser competitivos frente a otros *burós*, exigen que los oferentes les entreguen información completa y correcta.

En algunos países la información que los oferentes de crédito pueden transferir a los *Burós de Crédito* se limita a información

crediticia negativa. Es decir, información sobre incumplimientos e información referente a fraudes en la materia.

La desventaja de este enfoque es que al no incluirse la información positiva, es decir, información sobre los balances, aperturas de cuenta o límites de crédito, así como información referente a deudores cumplidos, se reduce significativamente la capacidad de evaluar el nivel de riesgo de los sujetos de crédito, ya sea que hayan o no tenido incumplimientos.

Estudios realizados de calificación de riesgos muestran que para un porcentaje de aprobación de solicitudes de crédito preestablecido la probabilidad de incumplimiento en el crédito otorgado aumenta notablemente al eliminarse del ejercicio de valuación la información positiva, similarmente el porcentaje de aprobación de solicitudes para una probabilidad de incumplimiento dada disminuye significativamente cuando la valuación se hace sólo con información negativa.

Es previsible que se obtengan resultados similares a los que se acaban de mencionar si los ejercicios de evaluación se realizan para *Buró de Crédito* que reciben información que un reducido número de oferentes de crédito y para *burós* con un gran número de oferentes. Las evaluaciones que se hagan para *burós* con mayor información serán más precisas y mejores.

Para un porcentaje de aprobación de solicitudes dado la probabilidad de incumplimiento es menor, similarmente para una probabilidad de incumplimiento dada el porcentaje de aprobación es mayor al crecer el número de oferentes que reportan información crediticia a los *burós*.

En la medida que los *Burós de Crédito* cuenten con información más completa, porque procesan información positiva y negativa y porque tienen información de un gran número de oferentes, los servicios que ofrezcan serán mejores y esto redundará en que el crédito se asignará de manera más eficiente en la economía.

Es por ello que la competencia entre *Burós de Crédito* no debe concebirse como una competencia que segmente artificialmente las bases de datos o los mercados de información crediticia, existen beneficios económicos considerables por juntar y agregar información, así como pérdidas considerables de que ocurra lo contrario.

Los beneficios de la competencia entre Sociedades de Información Crediticia debieran reflejarse en una creciente base de oferentes de crédito inscritos en los servicios de los *burós*, en menores tarifas, en un trato equitativo entre los distintos oferentes de crédito, en la utilización de tecnologías de punta y en una fuerte innovación de servicios.

La intensidad de la competencia del mercado de información crediticia depende de cómo se organice la industria. Esquemas que podríamos llamar de club de oferentes de crédito, en la que los *Burós de Crédito* son controlados por los miembros del club procuran modular la competencia y estabilizar las relaciones entre sus miembros, tienden a limitar el compartimiento de información con externos y tienden a segmentar el mercado de información crediticia.

En el caso de México de los tres *burós* originalmente autorizados a mediados de los años noventa, dos salieron del mercado principalmente por los obstáculos que tuvieron en acceder a la información crediticia bancaria.

Por otra parte, en el esquema de *burós* independientes, es decir, independientes de los oferentes de crédito, éstos procuran que sus servicios estén disponibles a cualquiera que quiera pagar por ellos, son altamente incluyentes debido a que contar con una amplia base de oferentes participantes se percibe como una ventaja competitiva y tienden a prosperar en mercados volátiles y dinámicos.

A manera de conclusión de estas ideas conceptuales podemos afirmar que la existencia de servicios de información crediticia eficientes conduce:

Uno. A fomentar el cumplimiento de obligaciones crediticias.

Dos. Reducir los costos de transacción en el mercado de crédito, pues en su ausencia los oferentes que incurren los agentes que requieren de este tipo de información, de lo contrario tienen que incurrir en mecanismos más oneroso para obtenerla, completarla o hacerla más precisa.

Tres. Asignar eficientemente el crédito en la economía.

Cuatro. Fomentar el crecimiento de la economía sobre bases sólidas.

Ahora me voy a referir a avances en México en relación al tema de la protección de la información crediticia.

Antes, quizás, hacer una mención de que al buscar un balance entre la privacidad y el comportamiento de información crediticia, el individuo toma en cuenta que si no permite al posible otorgante de crédito obtener un reporte de crédito de su persona, probablemente éste no va a otorgarle el crédito o se lo va a otorgar con tasas de interés elevadas.

Es por ello que al solicitar un crédito, el individuo generalmente acepta que el otorgante obtenga un reporte de crédito de su persona.

En México diversas leyes del sistema financiero obligan actualmente a las entidades financieras a guardar secreto de la información crediticia de las personas: La Ley de Instituciones de Crédito para bancos y fideicomisos, la Ley del Mercado de Valores para las casas de bolsa.

La violación del secreto financiero obliga a las entidades financieras a reparar los daños y perjuicios que se causen, sin perjuicio de las responsabilidades penales procedentes.

No existe una obligación de guardar secreto, equivalente para los oferentes de crédito que sean empresas comerciales.

La Ley para Regular las Sociedades de Información Crediticia del 2002 contempla diversas medidas de protección para los datos crediticios:

Uno. Transmisión de reportes de crédito a terceros, sólo con autorización expresa, mediante su firma autógrafa.

Dos. Calidad técnica, honorabilidad e historial crediticio satisfactorio de los consejeros y de los directores generales de las Sociedades de Información Crediticia.

Tres. Manuales operativos estandarizados, para el registro de la información por parte de los oferentes de crédito, que son usuarios de los servicios de las Sociedades de Información Crediticia.

Cuatro. Medidas de seguridad y control en las Sociedades de Información Crediticia contra el manejo indebido de la información.

Cinco. Sistemas y proceso para verificar la identidad de las personas, de quienes se solicitan los datos y de quienes acceden a los reportes.

Adicionalmente la ley otorga derechos a los titulares de los datos, mismos que voy a resumir:

Uno. El derecho de acceso a su reporte de crédito especial ante las Sociedades de Información Crediticia, en un plazo máximo de cinco días. También existe este derecho cuando la persona acude a los oferentes de crédito; ellos tienen la obligación de tramitar esta solicitud.

Dos. La solicitud y el acceso a los reportes de crédito puede darse por diversos medios: personalmente en las oficinas de las Sociedades de Información Crediticia, por correo, fax, correo electrónico, teléfono, Internet.

En el caso de que se solicite por Internet, actualmente el *Buró de Crédito* entrega el reporte de crédito especial en ese mismo momento, de manera gratuita.

Se han establecido tarifas máximas para garantizar el acceso de las personas a su información. La tarifa de acceso, como dije, es gratuita y las subsecuentes también son gratuitas, siempre y cuando se realicen en intervalos no menores a 12 meses.

Las Sociedades de Información Crediticia deben tener un número telefónico gratuito de atención al publico; las reclamaciones se pueden presentar directamente ante las Sociedades de Información Crediticia y se sujetan a un mecanismo claro y con plazos definidos.

En caso de que el otorgante de crédito no responda a la reclamación los *burós* deben efectuar las modificaciones solicitadas. Este procedimiento es gratuito para las dos primeras reclamaciones de cada año.

Se establece un plazo máximo de 84 meses para la retención de los datos crediticios en los *burós*, ya sean datos negativos o positivos.

A fin de mejorar la calidad de la información y que ésta reciba un tratamiento uniforme por parte de las Sociedades de Información Crediticia, éstas deben establecer formularios e instructivos de llenado para las empresas que les envíen información. Dichos formularios e instructivos deben ser dados a conocer al público.

Tratándose de una mesa que debe abordar también el tema de la mercadotecnia directa, cabe señalar que las Sociedades de Información Crediticia también pueden apoyar a empresas que deseen realizar actividades de mercadotecnia directa.

La regulación permite a empresas que son usuarias de los servicios de las Sociedades de Información Crediticia, obtener reportes de crédito, con el objeto de realizar ofertas de crédito a personas físicas, con las que no tienen contacto.

Las empresas interesadas en efectuar estas ofertas de crédito deben informar a las personas a las que dirigen sus ofertas, su identidad, las características del crédito que ofrecen, tales como tasas de interés y comisiones asociadas.

Tres. Obtener las autorizaciones por medio telefónico o Internet, para estar en posibilidad de acceder a los reportes de crédito correspondientes. Para estos casos se ha autorizado la sustitución de la firma autógrafa con un proceso de identificación de la persona, que incluye nombre y dos apellidos, domicilio, CURP o fecha de nacimiento, y últimos cuatro dígitos de ciertos contrato de crédito vigente.

Paso a la última parte de la plática. Los Retos. Si bien en las entidades financieras los datos personales crediticios, entre otros, están protegidos y las Sociedades de Información Crediticia protegen los datos crediticios que provienen tanto de entidades financieras como empresas comerciales, en la actualidad no existe una regulación de protección de datos crediticios que aplique a las empresas comerciales.

Después de casi 10 años de haber iniciado operaciones, el *Buró de Crédito* todavía no cuenta con la información de un gran número de oferentes de crédito no bancarios, como son empresas comerciales, e incluso las cajas de ahorro.

El reto es hacer que el mercado atienda eficientemente a estas empresas. Para ello es indispensable que exista el tipo de competencia entre Sociedades de Información Crediticia mencionado anteriormente.

En la actualidad existe un riesgo de segmentación artificial de bases de datos, lo que iría en detrimento del valor de los servicios que prestan las Sociedades de Información Crediticia y de su desarrollo.

La segmentación haría más difícil y costoso obtener historiales crediticios completos de las personas, con consecuencias, potencialmente perjudiciales sobre el mercado de crédito.

La industria de información crediticia pudiera conformarse por clubs de oferentes de crédito.

Los oferentes de crédito tenderían a participar solamente en el club al que pertenecen. Tanto el *Buró de Crédito*, como *Círculo de Crédito*, la otra sociedad de información crediticia recientemente autorizada, se asemejan a este esquema de clubs.

Varios bancos son dueños del 70 por ciento del *Buró de Crédito*. El porcentaje restante que corresponde a socios tecnólogos, mientras que el círculo de crédito está relacionado con empresas que atiendan estratos de ingresos medios y bajos.

Aparentemente existe interés también de las sociedades de ahorro y crédito popular en formar su propio *buró*.

El reto es crear un mercado de información crediticia incluyente, con *burós* en los que los oferentes de crédito tengan confianza plena de que la información que proporcionen es utilizada con total imparcialidad, y las tarifas son equitativas para oferentes chicos y grandes.

El esquema que probablemente conduce al más rápido desarrollo del mercado de información crediticia en México, es el de *burós* independientes sujetos a una estructura transparente de gobierno corporativo.

Esta es la tendencia que se observa en los mercados de información crediticia más desarrollados del mundo.

Por último, si bien actualmente el 94 por ciento de las personas en el *Buró de Crédito* son deudores cumplidos, la percepción que existe en la sociedad del mercado de información crediticia es frecuentemente negativa. Las Sociedades de Información Crediticia se perciben muchas veces como listas negras, en las cuales, naturalmente, hay que evitar estar.

No se ha hecho suficiente énfasis en que la gran mayoría de las personas se benefician de estar reportadas en los *burós*, pues ello les permite acceder a nuevos créditos en condiciones preferenciales.

Tampoco se ha enfatizado el balance positivo que para el mercado de crédito y el crecimiento económico del país está teniendo o puede tener el tercer participante integral en los mercados de crédito.

Moderadora: Isabel Davara Fernández de Marcos. Consultora especialista en Protección de datos personales.

Como les anticipaba, yo creo que esta mesa va a dar grandes temas, porque trata, en mi opinión, dos de los temas que generan más polémicas, específicamente las normativas en protección de datos, porque puede llevar a pensar en una confrontación entre las tendencias mercantilistas y las tendencias de protección de las garantías individuales.

Coincido con el doctor del Villar en que estas excepciones, en particular la de información crediticia que él mencionaba se hace en las normativas de protección de datos en beneficio del tráfico mercantil.

Mi pregunta es: ¿dónde está el balance, dónde está el equilibrio?

Mencionaba él, puede llegar a pasar que no se le dificulte obtener el trabajo porque la empresa que te va a contratar tenga tu historial crediticio.

¿Cómo podría ser eso? ¿Eso no sería una finalidad incompatible?

Juan Pablo Guerrero Amparán fue nombrado Comisionado del IFAI por el Presidente de la República y aprobado por la Cámara de Diputados del Congreso de la Unión para el período 2002-2009; ha concluido sus estudios de doctorado en Ciencia Política y política Pública en París, en el Instituto de Estudios Políticos; es maestro en Política Pública y maestro en Economía y Política Pública por la Universidad Hopkins, y sus principales áreas de especialización son las de presupuesto y finanzas públicas, reforma de administración pública, rendición de cuentas, servicio civil y descentralización fiscal.

Ponente: Juan Pablo Guerrero Amparán.

Yo quiero compartir con ustedes una reflexión que está claramente en proceso de construcción, por lo que mi intervención contrastará enormemente con lo ordenada y clara que fue la de Rafael.

Quiero sugerir que incorporemos en esta discusión otro elemento de la confianza, que tiene que ver también con la protección de la intimidad y con el conocimiento del otro, es decir, con el acceso a la información sobre su persona.

Voy a sugerir que la circulación, el libre flujo, el intercambio, la publicidad de datos personales genera confianza, genera certeza y esto favorece la cohesión social, los intercambios sociales, los intercambios económicos, los intercambios personales y desde luego las asociaciones económicas sobre las que no abundaré mucho, me seguirán en la palabra quien podrá hacerlo extensamente.

Debo hacer de entrada un deslinde institucional, lo que aquí planteo no forzosamente coincide con la posición del Instituto en el que tengo el gran honor de trabajar.

Lo que sí me voy a permitir hacer es compartir la experiencia que hemos tenido en el IFAI, que está encargado del acceso a la información pública y, por otro lado de la protección y el acceso a los datos personales y que vive semanalmente, pero muchos, los comisionados, cotidianamente el conflicto entre el principio de publicidad, el derecho a saber y el derecho a la privacidad.

El Estado, México no es la excepción, tiene las bases de datos personales más amplias y más delicadas y tiene la obligación de proteger esos datos personales. Pero es evidente que en ocasiones la publicidad que también es un mandato del Instituto merma la privacidad.

Los ejemplos que puedo referirles sobre la publicidad de datos personales cuando se relacionan a la regulación que el Estado hace sobre particulares tiene que ver con cuatro condiciones: El destino de los recursos públicos, las contrataciones, es decir, cuando el gobierno actúa como una contraparte económica, los privilegios por permisos que le permiten a particulares, permisos, autorizaciones, concesiones, actuar en condiciones excepcionales en su beneficio y las infracciones de normas federales.

En el primer punto, quienes conocen la Ley Federal de Transparencia saben bien que los sueldos, las remuneraciones, las prestaciones de todos los servidores públicos son públicas, pero no sólo eso, las becas, los subsidios directos personales, las ayudas también obligan al Estado a relevar el nombre y las condiciones en las que se reciben estos recursos.

Y en esto no solamente hay obligación de dar acceso sin mediar a una solicitud específica, sino que, como saben, está en Internet.

También se releva el nombre de la contraparte económica del Estado cuando éste es un agente de derecho privado, que además, como en la mayoría de los países, es el mayor actor en la economía.

Tanto en obras públicas, contratos, compras de bienes y servicios también se afecta el dato personal, el nombre, las condiciones generales del socio, aunque sea estrictamente temporal del Estado en una transacción económica.

Decíamos que también todos los beneficiarios de licencias, autorizaciones, concesiones, por ese sólo hecho tienen que renunciar a alguna parte de la privacidad de sus datos, referidos exclusivamente a esta actividad, pero también son sujetos de la luz a la que obliga la Ley Federal de Transparencia.

Y esta última condición la de la violación o infracción por normas federales no está planteada así en la ley como una obligación de transparencia que se ponga en Internet, pero es un criterio en el que el Instituto se ha pronunciado, aquí hablamos de normas sanitarias, normas ambientales, incluso,

quebrantos financieros en donde se ha planteado que en esas condiciones y una vez concluido el proceso de la autoridad el nombre de los sujetos de estas transgresiones es público.

¿Cuántas veces ha ordenado el IFAI que se entregue información que en un origen fue denegada con el fundamento de la confidencialidad? Innumerables.

Debo decir que ahí son los debates más intensos entre los comisionados y, sin duda, cuando se tocan estos dos principios, estamos ante los recursos y los casos más complejos.

No me voy a extender en las gráficas que ponían para ustedes un ejemplo, por ejemplo la siguiente en materia de autorizaciones, permisos y concesiones, identifican a las dependencias y entidades con mayores casos.

Allí están. Les digo que no me detendré, solamente, dado que el *pay* es muy difícil de leer, les digo que en Comunicaciones y Transportes, la Comisión de Telecomunicaciones, la Comisión Nacional del Agua, la Secretaría del Medio Ambiente representan cerca del 40 por ciento de los recursos, las quejas que hemos tenido, relacionadas con negativas originales que se fundamentan en la confidencialidad de un tercero, para negar la información.

Lo que quiero plantear, para luego hacer un símil o el razonamiento en el caso de los particulares es que, ya se ha dicho, la información sobre el Estado; la información entre el Estado y los particulares, entran en conflicto estos dos principios, el de la publicidad y el de la privacidad y hemos tenido tres formas de resolverlo.

En el caso de México, la Ley Federal de Transparencia se ha diseñado, entre otras cosas, pero enfáticamente en garantizar la rendición de cuentas, el acceso sencillo a la información del Gobierno y el cumplimiento de las reglas, la consolidación del Estado de derecho.

También se enfatiza la protección de datos personales, pero es, como bien saben, más bien frugal en ese tema, mientras que se extiende mucho, dado el objetivo, el mandato de hacer del Gobierno mexicano uno transparente, más honesto y más eficiente.

Pero volviendo a este conflicto y una vez establecido el mandato de transparencia, las tres formas de resolver el dilema ha sido, por un lado, que uno de estos principios, publicidad, privacidad, prevalezca sobre el otro.

Por otro lado, dar publicidad de datos personales que no son confidenciales y, finalmente, una versión pública.

Con relación al primero, un principio el de publicidad o el de privacidad prevalezca sobre el otro, pues siempre es un juicio subjetivo, es una instancia colegiada la del Instituto, y en muchas ocasiones, cuando están en conflicto estos dos principios, publicidad y privacidad, hay votos diferenciados.

Debo decir que en ninguna resolución el Instituto ha ordenado que se den datos relacionados con la intimidad de cualquier persona. Pero sí, sin duda, se ha ordenado que se den datos personales.

La segunda forma de resolución es cuando se trata de información que obra en registros públicos o fuentes de acceso público.

Debo decir que este artículo ha resultado providencial, para dar acceso particularmente a muchos beneficiarios de autorizaciones, concesiones y permisos, porque nos ha referido a registros públicos como el de la propiedad de sociedades mercantiles, de comercio, con lo cual la información que es denegada por el sujeto obligado el Instituto ha mostrado que en realidad ya obra en una fuente de acceso público, con lo cual éste ha permitido la revelación de la información.

Recientemente vivimos un caso que recibió interés público relacionado con el otorgamiento de permisos para casas de juego por parte de la Secretaría de Gobernación. El alcance de ese

acuerdo de apertura hubiera sido otro si no hubiéramos tenido este artículo.

Y finalmente, la tercera salida ante este conflicto es la elaboración de versiones públicas, ordenar que se den los documentos que acreditan la actuación del Estado en su relación específica con el particular, pero se protege información confidencial.

Y sobre eso es de mi agrado comentar con ustedes que ya ha habido una tesis de el Poder Judicial que favorece precisamente, legitima plenamente la elaboración de estas versiones públicas al establecer que no se afecta el interés jurídico del titular de la información cuando la resolución obliga a eliminar, previo a su entrega, la información sobre datos personales.

No me detengo sobre los beneficios de la publicidad. Es claro que cuando una Ley de Acceso a Información es realmente efectiva se transfiere poder a la sociedad, que puede cuestionar al Estado, le deben contestar, eso inhibe que se hagan trampas. También favorece la legitimidad, no solamente jurídica, la del apego a las reglas, sino favorece la legitimidad política de quien en forma transparente muestra que su actuación es buena, y desde luego favorece que haya confianza en los ciudadanos, porque obtienen mayores y mejores elementos de información, para la toma de sus decisiones personales.

Qué lecciones puede arrojar esta experiencia para la relación entre dos particulares o entre los particulares que no se conocen, obviamente, ese es el supuesto. Pero ya sea porque lo desean o porque tienen obligación, deben llegar a una forma de interacción de acuerdo.

Pues hay dos condiciones, o se apegan a las reglas establecidas que ya norman tratamientos, como el que van a llevar a cabo o se conocen, intercambian información sobre el asunto específico que los hace relacionarse.

Lo cierto es que en cualquier caso saber del otro, tener información, que alguien nos dé referencias sobre aquel que nos va a vender un auto, un bien inmueble, cualquier otra cosa o pretende una sociedad, de cualquier tipo, ayuda, genera confianza.

Es claro que el nivel de información que se va a intercambiar dependerá claramente del objeto de la relación que pretendemos tener con esa persona.

Propongo que a menor confianza hay mayor necesidad de información y a menor información con relación a mi interlocutor, a mi futuro asociado contratante, yo requiero pagar mayores costos para concretar la relación.

Y aquí, haciendo la analogía con lo que acabamos de ver, hay tres soluciones.

Por un lado la de asumir los costos de transacción y pues esto ya se ha analizado por expertos en la materia de la confianza en el sentido de lo que cuesta cuando no se tiene esa confianza mínima, establecer contratos que sean aceptables para los desconfiados, por una parte.

La segunda es compartir sólo la información necesaria que me ayuda a que mi interlocutor me tenga la suficiente confianza como para formalizar el contrato. Y esto, me he permitido en un exceso llamarle la versión pública personal, yo sé qué información le puedo dar sin que esto, y sólo la necesaria. Y finalmente obtener la información que ya es pública.

Aquí, terminó proponiendo que el intercambio de información favorece la responsabilidad en la decisión, es decir, nos responsabiliza de nuestras decisiones porque sabemos mejor a qué atenernos, facilita el contrato que será más realistas, más apegado a la verdad de cada cual y por lo tanto tendrá mayores posibilidades de cumplimiento, se incrementa la legitimidad no sólo por apego a las reglas del contrato, si no por la fama de quien cumple o no cumple los contratos, viene ahí la cuestión del prestigio que me parece tiene un enorme impacto en el orden social.

La sociedad se autocontrola por la importancia que cada quien otorga a su papel social, me parece que se favorece la certeza finalmente en los intercambios sociales y la confianza, lo cual genera bienestar.

¿Qué tiene que ver esto con una Ley de Protección de Datos Personales?

Me parece que debe reducir al máximo los costos para obtener la información que ya es oficialmente pública de las personas. Me parece que debe plantear claramente las reglas para establecer los mecanismos de las versiones públicas personales, es decir aquella información que el individuo está dispuesto a compartir para fines sociales específicos y, por supuesto y en primer lugar aquí el orden no significa, no tiene pues una implicación en la importancia, de proteger la intimidad.

La última lámina sugiere que a partir de estas consideraciones parece inevitable distinguir entre grupos de datos personales: los de la intimidad, los que plantean generalmente los pisos o lo mínimos de nuestras relaciones sociales para casos específicos y los que ya son públicos por ley.

Para cada tipo de dato personal debe definirse un principio y procedimiento de intercambio para los datos sensibles, el consentimiento expreso, de otra forma no podría intercambiarse para los no sensibles, aquellos que nos permiten esta versión pública personal, el consentimiento tácito o la oposición expresa y, finalmente lograr mayor accesibilidad para los datos que ya son públicos. Gracias por su atención.

Moderadora: Isabel Davara Fernández de Marcos. Consultora especialista en Protección de datos personales.

Es verdad, decías: la publicidad merma a la privacidad.

Son dos bienes jurídicos en conflicto, con lo cual como en cualquier Estado de derecho a veces entra en este conflicto y me arriesgaré a dada mi nacionalidad a no ensañarles a ustedes la famosa frase de: "*El respeto al derecho ajeno es la paz*".

Cuando la privacidad de la publicidad, su chamba, que es la difícil, es dirimir las fronteras de cual prevalece; pero no es un límite. La privacidad, los derechos de protección de datos no es un límite a la transparencia, no es un límite al acceso de información pública, no es un límite al mercado. Sí entran en conflicto, entonces, dirimen que son los que están para eso.

Carlos Alonso Martínez es licenciado en Derecho por la Universidad Autónoma de Madrid en 1985, es abogado en ejercicio, ha desarrollado su carrera profesional en Banco Pastor, Grupo Financiero Banesto y Grupo Equifax, donde actualmente presta sus servicios como Director de Asesoría Jurídica y Secretario del Consejo de Asociación Nacional de Entidades de Financiación ASNEF-EQUIFAX.

Realiza colaboraciones habituales con la Universidad Francisco de Vitoria, en el master de hecho bancario, con ICA en el master de hecho y tecnologías de información, así como con el master del Instituto de Informática y Derecho, adscrito a la Universidad Complutense de Madrid.

Ha sido participante en el III Encuentro Iberoamericano de Protección de Datos Personales, en Cartagena de Indias, Colombia.

Ha escrito varios libros y diversos artículos, entre sus libros destacan *La Guía Práctica de Protección de Datos Personales para el Marketing Directo*, *La Protección de Datos de Carácter Personal*, *El Consentimiento de Entidades Financieras y El Consentimiento Informado en Protección de Datos*.

Ponente: Carlos Alonso Martínez.

Yo en principio tenía idea de contar a ustedes y empezar un poco mi charla, que va a ser muy coloquial desde luego, contándoles lo que eran los *Burós de Crédito*, pero después de lo que ha

dicho Rafael del Villar, creo que muy poco más se puede decir de los *Burós de Crédito*.

Yo, no porque esté aquí en la mesa, sinceramente estoy muchas veces en conferencias sobre temas de solvencia, temas de crédito y para mí es una de las mejores exposiciones de cómo funcionan estos ficheros, los beneficios que tienen para el mercado, cómo se usan y cómo a su vez también revierten esos beneficios a los consumidores en la medida que pueden mejorar sus tipos de interés.

Para mí, desde luego, no sé para ustedes, les digo que ha sido sumamente interesante, ya difícilmente voy a poder contar lo que es un *Buró de Crédito* después de esa exposición.

Un poco la charla tanto de ayer, como de hoy, estaba escuchando las dificultades cómo muchos países entorno a esta conferencia en la que estamos participando, parece que tienen dificultad o miedo a poner leyes de protección de datos, dificultades, presiones de los sectores privados para ver cómo se va a poder cumplir, si esto puede en alguna medida dificultar la economía, es decir, cómo van a funcionar estas normas.

Y también se dio ayer un tema bastante interesante a mi juicio, que es un poco la discusión entre si es mejor la regulación o es mejor la autorregulación.

Yo una vez que no puedo contar ya demasiado sobre qué son los *burós* o al menos no debo porque también debo someterme al tiempo que marca la organización, bien entrar un poco a comentar la experiencia en España de cómo las compañías de solvencia, cómo los *Burós de Crédito*, es decir, qué ventajas, qué inconvenientes hemos tenido sobre la ley y si realmente esto para el negocio, no para el negocio o es algo que debe estar regulado.

En España la regulación que tenemos parte de la ley del año 92, denominada Ley Orgánica de Regulación del Tratamiento de Datos, LORTAD, y actualmente lo tenemos regulado en el artículo 29, de la Ley Orgánica de Protección de Datos de Carácter Personal, LOPD, una regulación bastante similar, aunque con algunos matices. Y la del año 92 vamos viviendo y conviviendo con esta legislación.

En España, el dato financiero, el dato de solvencia no se considera un dato sensible, por decirlo de alguna forma, no se considera un dato especialmente protegido, sino está asimilado a la afiliación sindical, a las tendencias políticas, al resto de datos especialmente protegidos, Pero es cierto que aunque no tiene ese carácter específico sí se reconoce que para el ciudadano evidentemente es un dato que tiene una especial sensibilidad el tratamiento.

Y en esta medida nuestra ley reconoce, por tres vía; repito, no es dato especialmente protegido, pero sí le da una cierta protección a este dato financiero o al uso del dato financiero.

Y básicamente y lo cuento a un nivel como suelo hacer siempre bastante práctico, lo hace por la vía de las sanciones, que normalmente es como entendemos la empresa privada cómo tenemos que cumplir las leyes, también ayer en algunas conferencias decía las dificultades en algunos países y la falta de mentalidad de cumplimiento de la norma que tenemos, pues, en España en cierta medida también nos pasa lo mismo.

Es cierto que legislaciones como medio ambiente, legislaciones como protección de datos difícilmente tuvieran el grado de cumplimiento que tienen actualmente, si no hubieran tenido atrás el aparato sancionador que ha motivado que las mismas empresas, en cierta medida, hagan esfuerzos para poderlo cumplir.

En concreto hace tres diferencias en el dato financiero, en el deber de información; mientras que cuando se incumple el deber de información, en cualquier tipo de dato personal es una sanción de carácter leve, 600 euros a 60 mil euros.

Sin embargo, cuando el deber de información se incumple en una empresa de solvencia, en un dato financiero, es una situación de carácter grave y, por lo tanto, entre 60 mil y 300 mil euros. Por lo cual la cuantía, evidentemente, sí hay una protección. Por eso quiero incidir en ello, no es especialmente protegido, pero no está desprotegido en absoluto.

Igual pasa cuando se incumple el deber de secreto, ese deber que tenemos todos los empleados que trabajamos en una compañía, los que manejamos esta información respecto a los datos, mientras en el contexto general de la ley es una infracción de carácter leve, nuevamente, cuando se trata de datos financieros o datos de insolvencia, es una infracción de carácter penal.

Y, a su vez también, en la regulación de medidas de seguridad, en el Reglamento de Medidas de Seguridad, los datos del sector financiero se encuentran en un nivel medio de seguridad; es decir, no en el nivel básico, sino que se les da un plus adicional de garantías de protección en cuanto a los aspectos de la seguridad de datos.

Ni que decir, tiene, que evidentemente sí lo digo, aunque no sea el objeto de esta charla, cuando son retos especialmente protegidos, las sanciones en todos los puntos que hemos tocado son de carácter muy grave y, por lo tanto, pueden llegar hasta 600 mil euros.

¿Cuál es esta regulación que ha habido en España para los ficheros de solvencia?

Básicamente, como he dicho antes, la tenemos en la LOPD, en el artículo 29, con tres aspectos a destacar, por decirlo de alguna forma.

Una es: Es una de las grandes excepciones a la ley, porque el acreedor, cuando son datos de cumplimiento o incumplimiento de obligaciones dinerarias, puede dar esta información sin el consentimiento del interesado. Nuestra ley, lógicamente, está regida por el principio de consentimiento y, sin embargo, aquí es una excepción.

La segunda características es que en el derecho de acceso hay, cuando un ciudadano ejerce su derecho de acceso a este tipo de ficheros, tenemos la obligación no solamente de dar la información de qué datos existen, sino que hay que dar las evaluaciones y las apreciaciones y, en suma, hay que dar todas las entidades que han consultado la información. Estos datos referidos a los seis últimos meses.

Esto evidentemente es una garantía para el ciudadano, porque no solamente le permite conocer cuáles son sus datos, si son iguales a los del fichero, sino que además tiene el derecho de conocer cuáles son las entidades que lo han consultado, de forma que ese control en el que insiste la sentencia del Tribunal Constitucional Español 292, que comentábamos también ayer, ese control de los datos, en cierta medida esta disponibilidad sobre su histórico de consultas, es una garantía para el mismo.

Por otra parte, también regula la ley el plazo de permanencia, debido a que en un país ya se regula cuatro años, hay algunos países en Europa con 10. La ley española optó desde el principio, desde el año 92, desde la primera ley, con un plazo de permanencia de seis años, que es un plazo que en principio se considera razonable y en España también acorde con los plazos que otras instituciones, como el Tribunal de Defensa de la Competencia habían manejado como plazos de permanencia para los ficheros de morosidad.

En concreto, el año 92, mientras Defensa de la Competencia habla de un plazo de cinco años, la nueva Ley de Protección de Datos en aquel momento reguló este plazo de seis años, que está considerado más o menos razonable por el sector como un plazo de permanencia para estos datos en los ficheros.

Adicionalmente a la ley, la Agencia de Protección de Datos en el año 95 dictó una instrucción en la que dio unas pautas de cómo debía de ser la información en estos ficheros.

Y evidentemente lo que vio allí fue un error más de calidad; normas de calidad en el sentido de que puso que debía tratarse de una deuda que fuera cierta, vencida, exigible, que hubiera resultado impagada y sobre la que la hubiera habido un requerimiento previo de pago.

Sí lo que hizo la Agencia Española de Protección de Datos en aquella instrucción, por una parte, fue realmente insistir en que en este tipo de ficheros lo que tenía que haber era deudas y deudas conforme a los criterios que nos marca el Código Civil.

Y, por otra parte, sí parece que una necesidad de que previamente el interesado, quien va entrar a este fichero, lo conociera o fuera requerido de pago, sino que el banco le metiera, sin que previamente hubiera habido ni siquiera ningún tipo de reclamación.

Esta notificación es adicional a la que tiene que hacer el responsable del fichero, en los 30 días siguientes a la inclusión. Por lo tanto, hay dos obligaciones: La de la entidad financiera o entidad que participa en el fichero requerida para entrar y obligación del responsable del fichero, de los 30 días siguientes de notificar la inclusión.

¿Qué problemas?, ¿qué ventajas ha habido de convivir con esta ley para los ficheros de solvencia?

Problemas gordos o problema graves ha habido dos. Uno de ellos fue que el cambio de la LORTAD a la LOPD, en que se cambió una palabra dentro del artículo 29 y no solamente del 29, sino también del artículo Cuatro, donde al hablar del principio de calidad se cambió "real" por "actual", llevó a una interpretación de que no se consideraba los saldos cero, es decir, cuando una persona debía, por ya había pagado. El saldo cero se consideraba que ya no podía estar en estos ficheros.

Esto posteriormente nosotros lo recogimos ante la Audiencia Nacional, que es el tribunal competente en España, y resolvió y confirmó que efectivamente ese cambio de esa palabra implicaba que el saldo cero ya no podría permanecer en este tipo de ficheros.

Nosotros, esto siempre ha sido una desventaja de la aplicación de la ley, tengo que decirlo como tal, porque creemos que realmente el saldo cero es beneficioso. Es beneficioso en el sentido, por supuesto sujeto a un plazo de permanencia, porque conlleva un poco, y esto da argumentación para mí, de Rafael del Villar, de que si no hay esta información este tipo de ficheros corre el grave peligro de acabar convirtiéndose en listas negras.

Sin embargo, cuando hay información negativa, está la información de la persona que incumplió, pero ya ha cumplido, ya va mejorando, ya no está en la lista negra.

Si además, añadimos la información positiva, o la información de las personas que cumplen adecuadamente sus compromisos de pago. El que evalúa el crédito tiene un mayor criterio y una mayor posibilidad de no condenar a muerte a la persona por el hecho de estar en un fichero de ese tipo.

En suma, puede ser que una persona tenga una incidencia con una compañía de telecomunicaciones en la que debe su acceso a Internet, debe decir dos cosas, pero después de esa persona se puede ver que tuvo una deuda de algo que pagó, y se puede ver que ha tenido ocho operaciones que ha cumplido correctamente con sus obligaciones de pago.

En su conjunto esa persona va a tener acceso al crédito. Si solamente está con una información meramente negativa puede tener dificultades.

Y esto es un poco la argumentación y la explicación también que yo quería, y en la que en mi opinión, desde luego, Rafael del Villar, cuando ha expuesto toda la información positiva ha sido absolutamente contundente y rotundo.

Esto en cuanto a los problemas, por lo tanto el saldo cero ha sido un problema y tenemos que

reconocerlo, y tenemos un problema con esta notificación de inclusión, porque algunos interesados niegan que la hayan recibido, con lo cual esa negativa implica lógicamente investigación por parte de la agencia, apertura de procedimientos.

Ahora mismo en eso se está trabando, y la solución parece que puede ir, de hecho ya está implantada, hemos empezado a implantarla, buscando que esa notificación no la hagamos nosotros, sino que la haga un tercero que sea auditable y que sea un medio independiente. De forma que podamos actuar en el marco de una prestación de servicios, y que un tercero garantice que todas las notificaciones, que en la práctica así se hace, cuando son puestas e identificadas al interesado.

Quería antes de terminar, simplemente hacer una mención a la posibilidad, una vez expuesto lo que es la regulación y los problemas, la posibilidad de autorregulación que argumentábamos. Para mí, y hablo solamente de los supuestos de solvencia, para mí no es una cosa opuesta a la otra, yo creo que debe de existir una normativa.

Pero yo creo que es muy difícil que una compañía de solvencia pueda convivir a su vez si no tienen una autorregulación, porque muchas veces las necesidades que tienes de acuerdos de regulación, de proteger; es decir, la norma hasta ahí, pero sensibilizar a los empleados y que todo el mundo en una compañía, en compañías multinacionales grandes que cumplan ese tipo de normativa no es fácil, con lo cual, muchas veces hay que poner medidas adicionales a las que pone la regulación estatal para sensibilizar a la organización, incluso muchas veces sensibilizar a los clientes y que todo el mundo llegue a un nivel de cumplimiento adecuado.

Les pongo, por ejemplo, actualmente el Real Decreto de Medidas de Seguridad en España no prevé una regulación de política de mesas limpias.

Puede parecer un tema absurdo e inocuo. Se puede decir que en el marco de una compañía de solvencia, en un banco, por supuesto también, en el sector financiero, una política de mesas limpias es absolutamente esencial, por el hecho de que nunca puede quedar un papel encima de la mesa.

Es decir, todo lo que lleva de orden, que no se puede destruir, un papel con información no puede ni con la papelera, que tiene que ser destruido. Todo ese tipo de políticas se llevan en la información y muchas veces nosotros que vivimos los problemas tenemos que también dar un paso por delante de la ley, ir aplicando esas políticas. Para mí esto en materia de solvencia es lo que es absolutamente favorable la autorregulación.

Para concluir la charla, yo les puedo decir mi opinión, llevo trabajando desde el año 95, prácticamente en el sistema de solvencia defendiendo a *burós*, representando en procedimientos y viendo un poco por la aplicación que tenemos con la Agencia Española de Protección de Datos y la Ley Española, yo creo que la experiencia es sumamente positiva.

Yo les diría que, egoístamente, un *Buró de Crédito* debe querer tener una Ley de Protección de Datos, porque una Ley de Protección de Datos marca perfectamente los límites de qué puede hacer, qué no se puede hacer.

Cuando no hay una regulación es muy difícil poder atender una reclamación de un consumidor, es muy difícil poder contestar. Evidentemente el argumento del consumidor es el de siempre, es el lógico y es el humano, el no quiero estar, quiero salir de ahí, y argumentos genéricos y es normal.

Una ley de protección de datos marca, primero, lo que pueda hacer una empresa de solvencia, los derechos del consumidor, cómo los puede ejercer y por lo tanto la valoración es sumamente positiva. Solamente esto tiene que ser completado con algo que es esencial, que tiene que haber una autoridad de control para regular todo esto.

¿Por qué? Porque evidentemente, y ahí sí tengo que poner mi defensa al sector privado. Es decir, yo no puedo competir en el mercado si tengo otra compañía de solvencia al lado pirateando información, dando todo tipo de datos y haciendo lo que quieran.

Yo puedo convivir con la ley española en la medida que tengo un órgano regulador que sé que va a regular a todo el mundo, que sé que va a incidir a todo el mundo, que nos inspecciona. Y es bueno que nos inspeccione.

Es cierto que a veces salen errores que hay que ir corrigiendo paulatinamente, pero que es esencial para poder avanzar, para poder competir en el mercado, ser competitivos, una ley que se aplique a todo el mundo igual, en igualdad de condiciones y que en el fondo todas las compañías si en un momento dado ya no tenemos saldo cero, no lo tenemos ninguno y todos podemos seguir compitiendo en el mercado.

No tenemos tanta información como antes, pero si la ley española considera que es como debemos funcionar en España, pues en otros países no es así. En Estados Unidos funciona con otra forma, en Inglaterra funciona con otra forma pero no queda más remedio que adaptarse a esa ley y en esa medida creo que la regulación y el hecho de una regulación es absolutamente positivo.

Moderadora: Isabel Davara Fernández de Marcos. Consultora especialista en Protección de datos personales.

No me dejaras mentir que en épocas tenías a un inspector en plantilla, casi le ponías silla al inspector en el *Buró de Crédito*, porque a principio las Sociedades de Información Crediticia, como las llaman, son las que más requieren adaptación o porque tratan quizás estos datos que tú llamabas, que se sentían sensibles por público. Y por supuesto coincido contigo en que la legislación te da los límites, las barreras.

Y otros puntos que haz tratado, que en mi opinión es esencial, es tanto la autoridad de control como la de las sanciones, porque en otras legislaciones de quizá no tanto nuestro entorno socio cultural, un ejemplo, a de Canadá no existe tratamiento de procedimiento sancionador, pero es que en Canadá son muy civilizados.

Países de nuestro entorno necesitamos más sanciones, decía el doctor Travieso que sólo cumplimos con la ley de gravedad. Digo, yo creo que cumplimos con la ley de las sanciones, somos quizás más divertidos, menos civilizados, más divertidos pero necesitamos esas sanciones y esos límites que impongan las autoridades de control y además las sanciones deben ser disuasorias porque sino, no olvidemos que a lo añadido tratar la información personal para las empresas supera el costo de la sanción y dice, bueno, pues voy a tratarlo mal, bien porque total puedo pagarlo. Hay que llegar a ese equilibrio.

Pasamos ahora a la participación de Hugh G. Stevenson que es director asociado para Protección Internacional del Consumidor de la Comisión Federal de Comercio de Estados Unidos; ha formado parte de las delegaciones de Estados Unidos ante diversos organismos internacionales, fungiendo como jefe de la delegación de Estados Unidos ante el comité sobre políticas de consumo de la OCDE; asimismo se ha desempeñado como moderador en varios grupos de trabajo de la FTC y de la OCDE, con énfasis en asuntos internacionales, incluyendo cuestiones de jurisdicción, resolución alternativa de controversias y Spam; ha realizado presentaciones ante comités legislativos, así como ante diversos organismos internacionales en los cinco continentes; encabezó los trabajos de la FTC en relación con propuestas legislativas encaminada a proteger al consumidor a nivel internacional; así mismo encabezó las negociaciones para celebrar acuerdos de cooperación con agencias de diversos países, tales como Australia, Canadá, Irlanda, España, Reino Unido y México.

Comparte también entre otros con el doctor José Luis Piñar Mañas de la Agencia Española de

Protección de Datos la cátedra de cursos sobre leyes de privacidad en Estados Unidos y Europa en la Facturad de Derecho de la Universidad de George Town.

Ponente: Hugh G. Stevenson.

Agradezco la oportunidad de darles mis perspectivas del modelo americano por el sector financiero, sectores financieros y comerciales.

Hablando como buen funcionario tengo que decir que mis perspectivas no son necesariamente la de mi agencia o sus comisionados.

Primero diré unas palabras sobre el sistema americano en contra de la privacidad más por lo general. En el sistema americano, debo decir que se ocupa y se preocupa mucho de la privacidad en particular en cuanto al sector al público y también en cuanto al sector privado.

En cuanto al sector público, el gobierno, tenemos varios derechos, incluso en nuestra Constitución, como es la Cuarta Enmienda contra las búsquedas irracionales; es importante comprender varias leyes desde los años 70 enfocadas en el tratamiento y acceso por el gobierno en cuanto a las carpetas gubernamentales sobre la ley de privacidad, en cuanto pedimento acceso a los datos de las instituciones financieras y en cuanto a los casos asociadas con el teléfono y la red, Electronic Communication Privacy Act, y también tenemos un acto en cuanto al acceso de la información pública.

En cuanto al sector privado regulamos ciertos sectores de la industria y ciertos tipos de datos, los más sensibles, donde hay la posibilidad, la más grande de daño a los consumidores, hay varias leyes y varias agencias encargadas con el cumplimiento de estas leyes, ejemplos son los datos financieros, nuestras agencias bancarias y el marketing directo y los datos asociados con la salud.

La FTC, mi agencia, es una de las agencias encargadas de la protección de privacidad, es una agencia federal a nivel nacional, es una agencia independiente con cinco comisionados, nunca más que tres de un partido político y es una agencia gubernamental.

Nos ocupamos de la competencia y la protección de consumidores y para nosotros en cuanto a la protección de consumidores somos más semejantes con PROFECO. Y una parte de proteger a los consumidores es proteger la privacidad, y hablamos de la privacidad de consumidores más que protección de datos como vocabulario.

Estamos encargados con varios tipos de responsabilidad que juntos protegen los intereses de los consumidores, se puede decir como una cultura del bienestar de los consumidores: primero hacemos reglas; segundo, discutimos la política relevante a encuentros como éste, encuentros públicos sobre muchos temas asociados con la privacidad. Tercero, tenemos un programa muy sólido que exige cumplimiento de la ley, y cuarto, alentamos la autorregulación de la industria, y por fin hacemos, que es muy importante, como ha dicho el propio Carlos Arce, hacemos educación de consumidores, de empresas y de industria. Para nosotros en cuanto a la protección de consumidores lo importante es el bienestar, incluso, el bienestar económico de los consumidores.

El bienestar de los consumidores es nuestro punto o la piedra de toque, y con este punto comprendemos que la subrogación de datos tiene un valor para los consumidores.

Las empresas pueden ofrecer una elección más grande de productos, de servicios, de métodos de pagos y la información es muy importante para el mercado de crédito, muy importante porque baja las barreras contra la competencia, y más competencia es mejor.

Al mismo tiempo, claro que hay situaciones con problema de privacidad, de seguridad, de mal uso

de los datos, con posibilidad de daño. Hay un balance como hemos visto con privacidad, hay muchos balances, como nuestro moderador ha dicho: ¿dónde está el equilibrio?, hay muchas preguntas así en cuanto a la privacidad.

Como se ha dicho, por ejemplo, con la libertad de expresión, con la lucha contra el terrorismo y aquí en contra del mercado. Y se le ve también en los documentos con líneas directrices de la OCDE, el marco legal de APEC.

Tenemos en los Estados Unidos varias leyes en cuanto a los datos financieros, mantenemos el Fair Credit Reporting Act, FCRA, la Ley Federal de Informe Justo de Crédito de 1970, con varias enmiendas. Es una ley bastante sofisticada y es el balance. Se aplica a las agencias privadas que recolectan información con respecto a las transacciones de crédito de los consumidores. Y recolectan información laborable tanto como información negativa.

Permite a las agencias de crédito compartir esta información, pero solamente en ciertas circunstancias, por ejemplo, si el consumidor da permisos, si es necesaria para una transacción de crédito.

Tenemos también una ley que establece normas preventivas para el manejo eficaz de los bancos de datos personales, y prohíbe a las instituciones financieras revelar ciertos datos personales de sus clientes a entidades sin su permiso.

Tenemos recientemente reglas ofreciendo medidas de salvaguarda. Las reglas se aplican a las instituciones financieras, a los bancos, por supuesto. Pero también a otras entidades que tienen bases de datos financieras de consumidores. Por ejemplo, empresas que ofrecen tarjetas de crédito o hipotecas y también agencias de informes de crédito. Es importante destacar más generalmente la ley contra las prácticas engañosas y desleales. Hemos percibido casos cuando hay una brecha de una promesa relevante a la política de privacidad. Hemos perseguido casos contra Microsoft.

Nuestra agencia persiguió casos contra una práctica considerada como desleal, cuando la empresa no ha tomado medidas razonables para proteger los datos de sus clientes con esta ley la Federal Trade Commission Act., FTC, Comisión Federal de Comercio.

También apoyamos la idea de una ley recogiendo medidas de salvaguarda para todas las empresas en cuanto a ciertos datos, requisitos de notificación, cuando hay una brecha, cursando un riesgo significativo de robo de identidad.

Tenemos también varias actividades en cuanto al robo de identidad.

En cuanto al marketing directo, establecimos el *National Do Not Call Registry*, *No Llame*; es semejante a algo que el doctor Arce comentó esta mañana.

Con ello los consumidores tienen control sobre las llamadas de telemercadeo que desean recibir en casa, y hubo un caso, debo de subrayarlo, porque se debe considerar en los Estados Unidos, por lo menos, también la libertad de expresión; hay un balance, hay una atención.

Pero nuestra regla ha ganado y hay ahora más de 100 millones de números registrados en esta lista. No estoy perdido en la traducción en este momento; más de 100 millones de números reconocidos, registrados en el padrón. Es interesante cómo hay conciencia de la gente en los Estados Unidos de por lo menos este derecho de privacidad; en comparación hay, como se ha discutido, un informe por la Comisión Europea sobre la conciencia de la gente. En Europa hay un tercio que conoce, que sabe que hay una Agencia de Protección de Datos y un tercio que saben que se puede tener acceso a los datos.

Y para nosotros este ejemplo es muy importante, porque es un éxito, por supuesto, pero también porque es un ejemplo de privacidad práctico, enfocado en el bienestar de los consumidores.

Y por fin hay el desafío contra el Spam. Hemos perseguido, hay muchos abogados en la FTC que hemos identificado más que 70 casos de Spam en los tribunales federales de los Estados Unidos, por lo menos, y también había varias casos asociadas con vínculos internacionales en cuanto a Spam. Y en esta materia hemos perseguido las prácticas, por lo general, engañosas. Tenemos también algo que se llama the Can-Spam Act.

Pero por lo general nuestra experiencia es que el desafío no es encontrar el delito o el malo, y el Spam es también un ejemplo de la necesidad de cooperación internacional. Como Jesús Rubí, de la Agencia Española ha dicho.

Y por eso tenemos que comprender otros sistemas. Hemos trabajado en la FTC con muchas agencias, por ejemplo, la Agencia Española de Protección de Datos, la PROFECO y con nuestros colegas en CONDUSEF en México. Y creo que eso es muy importante no sólo para la cooperación del cumplimiento de la ley, pero también para comprender mejor cómo funcionan los otros sistemas en el mundo.

Moderadora: Isabel Davara Fernández de Marcos. Consultora especialista en Protección de datos personales.

Cuando, cada vez que se invita a alguien a explicar la posición estadounidense que se intenta confrontar con la posición europea y el resto de países del mundo añadidos a la posición europea, tengo que decirle, no sin sentirme un poco mal al agradecerle todas sus menciones a mis intervenciones, que yo no creo que sean dos regímenes equiparables, porque coincido con lo que se expresaba ayer, no se puede comparar la autorregulación con la regulación.

Entiendo que la tendencia europea de regulación no puede ser equiparable a las tendencias autoregulatorias y regulatorias sectoriales que ustedes han mencionado.

No obstante creo recordar un informe de su propia organización en el 2000 en el que había un voto de tres comisionado a favor y dos en contra a favor de una regulación. Pero me voy a permitir augurar que los acontecimientos del 2001 desgraciadamente han supuesto un freno importante a la lucha a favor de la privacidad en el entorno norteamericano. Esas cosas también hay que tomarlas en consideración, aparte de los dos regímenes.

Rafael Adrián Avante Juárez es abogado por la Escuela Libre de Derecho con mención especial con la Tesis Profesional: *Aspectos jurídicos del gobierno en la Ciudad de México*; diplomado en el ITAM en Economía Aplicada, actualmente cursa su maestría en Derecho en la UNAM y miembro del Ilustre y Nacional Colegio de Abogados desde 1998: Profesionalmente se ha desempeñado en la Honorable Cámara de Diputados del Honorable Congreso de la Unión en LV Legislatura; en la Comisión del Distrito Federal como secretario técnico; en el Partido Revolucionario Institucional, en el Comité Directivo en el Distrito Federal, como asesor jurídico del Presidente del citado Comité; en la Procuraduría Federal del Consumidor como director general Jurídico Consultivo durante seis años; en la Secretaría de Comunicaciones y Transportes como secretario particular adjunto del secretario; en la Procuraduría Federal del Consumidor como subprocurador de Servicios al Consumidor; actualmente se desempeña como director general Jurídico Consultivo en la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF).

Ponente: Rafael Avante.

De no ser por la cantidad de asuntos que he tenido que atender en CONDUSEF, Rafael, Juan Pablo y Carlos casi me convencen del enorme privilegio que representa para uno estar dado de alta en el *Buró de Crédito*, pero ahorita entramos a revisar el tema a ver si realmente es tan bondadoso.

Empezaré rapidísimamente compartiendo con ustedes una breve teorización del gran tema de la protección de los datos personales.

Me parece esencial, con estas nuevas tendencias de la argumentación jurídica donde se habla esencialmente de valores y principios identificar un poquito qué traemos en juego y qué estamos pretendiendo cuidar en este gran tema.

Encuentro dos principios:

Al primero le llamaría de la *secrecía* y al segundo, le consideraría de la publicidad relativa de la información personal.

Por lo que se refiere al tema de la *secrecía*, los valores que están *in situ* son, por un lado, la libertad, decidir a quién y cómo voy a entregar mis datos. Y el valor por supuesto de la intimidad.

Por lo que se refiere a la publicidad relativa me parece que están en juego los valores de la transparencia y del acceso a la información, y no estoy hablando de la información pública.

Estos valores enfrentan sus desvalores, sus perversiones en términos aristotélicos y es aquí donde debemos empezar a poner el énfasis para cuidar cómo debemos normar y proteger esto.

La intimidad y la *secrecía* no pueden considerarse como una herramienta o como un obstáculo para que pueda yo valerme de esos principios para caer en la clandestinidad, en la mala fe, en el dolo o en la ilicitud. Cuando lo que pretendo es ocultar información valiosa para un tercero que me va a generar una ventaja inequitativa, hay un riesgo.

De la misma forma la publicidad relativa de la información, y conste que digo relativa porque no a todos y en todo caso, por eso es relativa, estamos hablando del sujeto privado, del individuo, también presenta su perversión.

Yo no puedo, valiéndome de ese derecho a obtener información tuya, caer en figuras de espionaje, prácticas comerciales agresivas y actos de molestia no autorizados o ilícitos. Ese es el otro lado, la otra perversión que se puede dar.

Los abusos de estas dos figuras son los que nos obligan a ser muy inteligentes para colocar un punto intermedio, y cuidar también los efectos que tendrá la regulación que le demos a estos dos elementos.

Paso entonces a compartir con ustedes algunas preocupaciones muy importantes que en CONDUSEF tenemos sobre el tema de los datos personales. Y el primero, claro, va referido al *Buró de Crédito*.

Me parece fundamental que el sistema financiero tenga un sano desarrollo, y me parece correcta la apreciación en el sentido de que una adecuada calificación crediticia, sin duda, impacta en el costo del crédito y es benéfica. Pero debemos tener cuidado, porque suceden varios elementos paralelos que no son tan benignos.

El primero de ellos tiene que ver con, no se trata de que me pongas la letra escarlata y el sambenito, que de aquí en adelante me vuelvo personaje macabro de las finanzas porque me pusiste un tache en la lista.

Me parece que debemos cuidar esto, porque además no olvidemos que esto no se restringe al tema del otorgamiento del crédito, lamentablemente.

Nosotros hemos identificado en CONSUSEF ya casos muy claros en los que se le está pidiendo a un individuo que solicita empleo, que exhiba su certificado, su reporte de crédito especial. Y por supuesto el usuario a mí me dice: Oiga, licenciado, necesito trabajo para pagar lo que debo, pero no me dan el trabajo porque debo. Nada más dígame entonces qué voy a hacer, primero.

Segundo, quién decidió que voy a llevar un tache. Porque a mí nadie me dio el criterio de calificación. Resulta que hay taches, medias palomitas, palomitas, menciones especiales o menciones desagradables. Pero esos números, esos números son altamente revisables y me parece que tenemos que ser muy cuidadosos en la posibilidad de que esa calificación, porque es

como una boleta de calificaciones no sean tan radical en muchos casos.

Igual las reglas o la normatividad interna de las instituciones financieras a partir de las cuales califican la cartera deben ser menos radicales en el tratamiento que dan a estas calificaciones.

Por el otro lado, se habla mucho en este tema del derecho al olvido, que es fundamental, por este sambenito del que hablábamos; al menos quítamelo algún día.

El tema está en que el derecho al olvido nos parece que toda vez que está tutelando al usuario debe versar sobre la información negativa, no sobre la positiva. Porque si a lo siete años vamos a borrar todo, entonces también el buen historial crediticio se fue. Entonces, más que un derecho al olvido es una prescripción de un registro, y entonces habría que ponderar este tema.

Finalmente en el aspecto del *buró* me parece muy interesante, muy atendible, y nosotros aplaudimos mucho la iniciativa que el *Buró de Crédito* ha tomado para notificar a las personas cuando alguien está solicitando su reporte de crédito especial, porque esto nos va a permitir de una manera muy estratégica, atacar el problema que también nos interesa mucho, y que ahorita lo voy a mencionar, del robo de identidad.

El robo de identidad está hoy perpetrándose de muy diferentes formas. Pero una de ellas es obteniendo la información crediticia de alguien, para saber cuál es el nivel de solvencia y para saber dónde no tiene contratos de crédito, para poder celebrarlos en su nombre.

Por eso esta iniciativa de *Buró de Crédito* la aplaudo enormemente.

¿Qué otra cuestión nos preocupa? Hablábamos de que una de las perversiones de este derecho a la intimidad o de la secrecía radica en ocultar información, que a veces puede resultar dolosa o a veces puede resultar clandestina.

A veces, a lo mejor es simplemente un silencio conveniente. Nosotros estamos participando activamente en una iniciativa ante la Comisión Nacional de Seguros y Fianzas, porque queremos crear una base de datos de registros de personas aseguradas, cosa que en España, entiendo se acaba de autorizar. El propósito fundamental es que existen muchos usuarios de contrato de seguro que cuando el asegurado, mejor dicho, beneficiarios de contrato de seguro que cuando el asegurado fallece ni enterados están que existía la póliza, mucho menos que había algún beneficio a su favor.

Y hoy no hay forma de accesar a esa información. Entonces, es un ejemplo de cómo a veces sí necesitamos accesar a cierta información, porque sí tiene un fin útil y benéfico. En ese caso, que se cumpla la voluntad del asegurado, porque en ocasiones y a algunos de ustedes les habrá sucedido, reciben incluso con su estado de cuenta de la tarjeta de crédito o reciben con los boletos de avión de un viaje determinado, que están protegidos con una póliza de seguros que los ampara por tales o cuales circunstancias, incluyendo el seguro de vida.

Nada más que no lo compartieron con nadie; nadie sabía que existía ese seguro y mañana no hay forma de accesar a esa información, para que sus beneficiarios puedan cobrarlo.

Un tema que me parece de la mayor relevancia. Estamos hablando de la libertad de decidir cuándo y cómo se proporcionan mis datos, y mucho se ha hablado aquí de la importancia de la autorización expresa del titular, para que los datos sean compartidos con terceros.

Bien. Si vamos a entrar a este nivel de tutela, me parece muy importante que evitemos el condicionamiento de la prestación de un servicio al otorgamiento de ese consentimiento; es decir, este consentimiento expreso tiene que ser absolutamente libre.

Si ya la legislación que protege a los consumidores y a los usuarios en muchos aspectos regula que no se puede condicionar la

venta de productos; yo no te puedo condicionar la venta de un litro de leche, a cambio que de me compres un kilo de jamón.

Me parece también muy importante que yo no pueda condicionarte la prestación de un servicio a que me autorices expresamente a compartir tu información con terceros, más aún, cuando esta autorización se incorpora dentro de un contrato por adhesión, en el cual ya mucho ha dicho la doctrina de lo cuestionable que puede el consentimiento, respecto de las cláusulas accidentales de un contrato de esta naturaleza.

Entonces, nos parece fundamental regular esta parte, para evitar que tanta tutela al consentimiento expreso se vea afectada por una práctica comercial.

Y en este mismo asunto nos preocupa de sobremanera la existencia de prácticas comerciales agresivas frente al usuario.

Yo no sé cuántos de los que están aquí presentes han recibido un sinnúmero de llamadas telefónicas de diferentes instituciones financieras, ofreciéndoles diferentes modelos, tipos y productos de tarjetas y de créditos personalizados.

Bueno, yo he visto casos y a la mejor hay alguno por aquí, en el que reciben la tarjeta. Ya olvídense de la llamada, llega a su domicilio el plástico. Me parece una cuestión muy delicada.

Y si vamos a tutelar la protección de datos personales, no cabe la mejor duda que si alguien recibió una tarjeta, un plástico, es porque se valoró su condición crediticia. Y entonces es la mejor prueba de que se obtuvieron ilegalmente sus datos personales.

En esos casos habría que exigirle a la institución financiera que nos demuestre el documento donde los autorizamos o donde se nos proporcionamos. Si no lo tiene, si no hay un consentimiento expreso para haber obtenido esa información nuestra, bueno, pues allí hay un tema muy interesante de responsabilidad.

Y finalmente otro de los aspectos que nos parecen muy delicados tiene que ver con las transacciones electrónicas. Aquí hay un dato personalísimo: La contraseña.

Este dato, definitivamente todos vamos a coincidir, es un dato que no puede ni debe jamás exigirse ni proporcionarse ni autorizarse que se proporcione a nadie, salvo al beneficiario.

Sí, nada más que nos estamos olvidando de regular adecuadamente, castigar severamente y proteger al usuario de las prácticas ilícitas que pretenden al obtener esta información.

Y muy claro está el caso en el que actualmente los *hackers o crakers* se introducen en la computadora del usuario, se hacen pasar por la institución financiera y obtienen la información.

Igual el tema del "*figing*", donde de manera fraudulenta, a través de artificios pretenden hacerle creer al usuario que son un banco y que requieren esos datos para que éste se los proporcione.

Al respecto quiero hacer un reconocimiento a la FTC, porque la página de Internet con la información que despliegan sobre seguridad en transacciones electrónicas, me parece valiosísima y muy interesante.

En esencia y por la poca disponibilidad del tiempo, yo me quedaría allí. Baste con hacer una recomendación a las instituciones financieras, en el sentido de que la competencia no se da en la comercialización agresiva, sino en la calidad el servicio.

Genera en su propia demanda, siendo eficientes en sus servicios y no los fuercen a contratar.

Moderadora: Isabel Davara Fernández de Marcos. Consultora especialista en Protección de datos personales.

Magnífica exposición y tiene un montón de usuarios aquí. Yo soy una de ésas a las que han llamado repetidamente.

Levanté mi teléfono, me dijeron que había sido agraciada con no sé qué, no seguí escuchando, y la casualidad, debo ser muy afortunada, que en mi otra línea de teléfono también había sido agraciada con el mismo premio.

Es muy fácil ponerte del lado del usuario porque por lo mismo, todos lo somos, pero es que en realidad, Rafael, los usuarios no siempre somos inocentes; haz puesto el ejemplo de las aseguradoras, decías que en España se han creado estas bases de datos de aseguradoras, sí, pero puede ser una situación parecida a los *Burós de Crédito*. Una de las razones por las que se han creado estos bancos de datos es porque existía una limitación en la ley que decía, hasta que usted saque un seguro, hasta 60 mil euros, no tiene que pasar un seguro médico, no tiene que pasar reconocimiento médico.

¿Qué pasaba? Llegaba un señor con una enfermedad terminal y se hacía diferentes seguros médicos hasta 60 mil euros sin reconocimiento médico.

¿Qué creaba eso? Bolsas de fraude en el mercado. Como no se podía cruzar no se podía saber quién tenía muchos seguros médicos que hubiera soltado la alarma y diría: este señor está intentando defraudar. Y no olvidemos, las instituciones financieras y las aseguradoras no pierden dinero, lo que concebían, elevaban las cuotas, las pólizas y sufríamos todos los que sí éramos inocentes.

Entonces, ponerse de lado siempre de los usuarios, no hay que llegar a extremos, digo, es muy fácil porque todos lo somos, y a mí también Carlos y Rafael casi me convencen de que quiero estar en el *buró*, porque de verdad sí quiero. O sea, si yo pago bien quiero estar en el *buró* porque es lo que están diciendo, quiero tener mi historial crediticio de manera que me traten bien.
En Estados Unidos y Carlos lo contaba, muchas veces le he oído decir, tienen estas listas, es difícil entrar al *buró* y hasta que no tienes un historial positivo nadie te da una tarjeta de crédito. Y me contaba siempre un episodio de los Simpson en la que al padre nunca le daban una tarjeta de crédito porque nunca tenía un crédito, con lo cual no podía tener medio de pago.

Y me decía Carlos: ¿Qué es mejor sólo un positivo, que te obliguen a tener un historial positivo para que te den crédito o que no te lo den si tienes un historial muy negativo?

El panorama es complejísimo, como mi misión es meter debate, pues te lo doy también a ti como al resto. Pero te digo, de parte de los usuarios es muy bonito y es muy fácil en el sentido de que todos lo somos y además, tienes toda la razón en los ejemplos que has puesto, porque yo podría haber ido gratis a Acapulco 500 veces. Pero hay que lograr el equilibrio de las dos partes.

El doctor Alfredo Reyes es, además de excelente amigo y un experto en la materia en todo lo que es nuevas tecnologías en derecho, es Presidente de la Asociación Mexicana de Internet, director jurídico de E-business en el Grupo Financiero BBVA Bancomer, doctor en Derecho por la Universidad Panamericana, postgrado en Dirección de Empresas en el Instituto Panamericano de la Alta Dirección de Empresa, profesor titular de Contratación Electrónica, maestría en Derecho de Empresas en las Facultad de Derecho de la Universidad Panamericana, catedrático de la materia Tecnologías de Información, problemas legales en la maestría en Comunicación Social de la Universidad Panamericana, profesor del Área de Comercio Electrónico, doctorado en Derecho del Instituto Tecnológico de Monterrey, profesor de Informática Jurídica de la Facultad de Derecho del TEC, Campus Ciudad de México y Campus Estado de México; integrante del grupo impulsor de la legislación en materia de comercio electrónico y del grupo de trabajo de banca y comercio electrónico en la Asociación de Banqueros de México y, autor entre diversas publicaciones, del libro *La firma electrónica en las entidades de certificación*, publicado por la editorial Porrúa en 2003.

Ponente: Alfredo Reyes.

Y la idea es platicar sobre la perspectiva del sector financiero y comercial.

Quiero partir de que, y ya lo hemos expresado aquí, en la legislación federal mexicana ya contamos y encontramos algunas disposiciones vigentes sobre la materia.

Ya el doctor del Villar se refirió, muy bien por cierto, a la Ley Federal de Sociedades de Información Crediticia. También ha habido referencias aquí en este mismo foro, en relación a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, donde hace poco se publicaron también ya los lineamientos sobre protección de datos personales.

Las últimas reformas a la Ley Federal de Protección al Consumidor, la regulación en materia de bases de datos por la Ley Federal de Derechos de Autor, muchas otras. Y en este sentido también las disposiciones jurídicas que regulan a las distintas entidades del sector financiero cuando establecen la obligación de recolectar, procesar y conservar ciertos datos personales de su clientela para prevenir la comisión de ciertos ilícitos, como pudieran ser el lavado del dinero o el financiamiento al terrorismo.

Aunado a lo anterior yo creo que también es muy importante considerar la posición de México en el ámbito internacional, porque si bien es cierto que tenemos celebrado un tratado de libre comercio con la Unión Europea, también tenemos celebrado un tratado de libre comercio con Estados Unidos, nuestros socios comerciales.

También ya Hugh hacia referencia a la OCDE y a APEC, que son convenios y tratados internacionales, que de alguna manera también hemos suscrito, y son también de acuerdo al artículo constitucional legislación en México.

Vamos entonces a referirnos en específico a una iniciativa, a una iniciativa de Ley Federal de Protección de Datos Personales, que fue presentada por el senador Antonio García Torres, del grupo parlamentario del PRI, en la sesión de la Comisión Permanente del miércoles 14 de febrero de 2001.

Se van a preguntar por qué hago referencia en específico a esta fecha, porque de hecho estamos hablando de una normativa que tiene ya más de cuatro años de antigüedad, que en muchos de sus conceptos ya ha sido superada en otros países.

Esta iniciativa fue dictaminada por las Comisiones Unidas de Puntos Constitucionales y de Estudios Legislativos de la Cámara de Senadores. Este proyecto de ley fue aprobado y publicado en la Gaceta Parlamentaria del Senado de la República el 30 de abril de 2002. Teniendo como objetivo principal el reglamentar las bases a las que estarán sujetas las personas y empresas propietarias de archivos y bases de datos, así como guardar el equilibrio entre sus derechos de uso, comercialización o transferencia respecto de su titularidad y los derechos de privacidad de los individuos.

En septiembre de 2002, esta iniciativa se turnó a la Comisión de Gobernación y Seguridad Pública de la Cámara de Diputados, y en octubre del mismo año se turnó a la Comisión de Comercio y Fomento Industrial, hoy Economía.

La entonces Comisión de Comercio de la Cámara de Diputados en noviembre de 2002 presentó al pleno un comentario aduciendo que el contenido de esta iniciativa resulta poco claro, ambiguo y su alcance e interpretación genera confusión.

De los estudios realizados, comenta dicho proyecto legislativo, produciría grandes afectaciones al comercio y al empresariado en general de nuestro país. Ojo. Hay que tener en cuenta que estamos hablando de la de 2000.

Quiero hacer referencia en específico a las reformas a la Ley Federal de Protección al Consumidor. Como ustedes perfectamente

saben, y seguramente ya se han comentado en este Encuentro, la fracción primera del artículo 76 bis de esta Ley Federal de Protección al Consumidor, impone una obligación a los proveedores, entre ellas es mantener la confidencialidad de la información, y la prohibición de difundirla o transmitirla a otros proveedores, a menos que el consumidor lo haya autorizado por escrito, o existe, en su caso, algún requerimiento de autoridad.

Asimismo, hay otra fracción en donde se impone al proveedor la obligación de mantener segura y confidencial dicha información, e informar al consumidor sobre las características generales de los elementos técnicos de seguridad y confidencialidad disponibles antes de la celebración de la transacción.

Quiero aclarar que no es que en el ámbito comercial o en el ámbito financiero estemos en contra de regular la protección de datos personales. Lo que quiero aclarar es que la iniciativa, la iniciativa que estamos ahora dictaminando en la Comisión de Gobernación de la Cámara de Diputados adolecen de algunas fallas o algún tipo de cuestiones que creo que pudieran ocasionar algunos problemas a la industria en particular de nuestro país.

En particular considero que la iniciativa debe pretender la regulación de la protección de datos de las personas físicas, recopilados, almacenados y procesados en archivos, registros y bases de datos de empresas del sector privado.

Estoy consciente de que las disposiciones regulatorias deben de guardar un sano equilibrio entre el derecho de protección y las obligaciones y demás disposiciones relacionadas.

Debemos de considerar también libertad de expresión; debemos también de considerar las cuestiones relativas a regulación, en materia de protección, combate al terrorismo, lavado de dinero, combate al narcotráfico o alguna orden judicial.

Vámonos a las principales preocupaciones respecto de esta iniciativa.

Ya el Comisionado Juan Pablo Guerrero hacía referencia a la distinción entre dato sensible, dato no sensible y dato público por ley, y en este contexto habría que modular lo que establece la iniciativa, porque la iniciativa de inicio establece un esquema a rajatabla en cuanto a *óptimos*.

Obliga a las empresas a obtener el consentimiento previo y expreso de los individuos, para poder enviar información.

Por otro lado tenemos, y ya se ha tratado también, la prohibición al flujo transfronterizo de datos personales.

En este sentido, tenemos un problema grave como empresas, porque si por un lado tenemos este principio en nuestra legislación, tenemos con nuestros socios comerciales, con el Tratado de Libre Comercio con América del Norte, también la prohibición de poner trabas al libre flujo de datos personales.

Seguramente me va comentar Isabel, yo en este sentido lo entiendo, que también tenemos un Tratado de Libre Comercio con la Unión Europea y en el mismo se hace referencia a manejar lo dispuesto por la Directiva, en cuanto a protección de datos personales.

Estamos en medio del sándwich en cuanto a México.

Por otro lado, tenemos el registro y entrega de bases de datos. En este sentido, la cuestión del registro y la base de datos de las empresas o registro y bases de datos en particular, también suponen cuestiones muy particulares, ¿qué entendemos por el registro y qué entendemos por la conservación o la entrega en su momento o en su esquema, de bases de datos?

Actualmente se manejan esquemas de Data WareHouse y se manejan esquemas muy

particulares; es decir, se habla de minería de datos o se habla de minería en cuanto a obtención de determinados "*kueris*" para obtener una información en particular y hablamos de cubos de información.

¿Qué es lo que vamos a registrar: El cubo de información madre, matriz o vamos a registrar el "*kueri*" con el que generamos la información, que tiene una vigencia muy pobre? La verdad es que estamos hablando que es una campaña en específico.

Si quieren que para cada una de las campañas estemos registrando, la verdad es que nos va salir carísimo. Dos, vamos a requerir una maquinota para poder guardarlas.

Otra, el registro de quiénes son las personas que tienen que ver con el manejo de la información en particular o con esa base o con ese "*kueri*", también va significar un problema bastante serio.

Otro punto importante es las facultades discrecionales a la autoridad, con el fin de definir la tecnología a emplearse en el manejo de archivos.

Quiero aclarar: Ya Hugh Stevenson hacía una referencia en específico a medidas razonables. Una cosa es medidas razonables y otra cosa es en específico imponer una tecnología.

Y a mí en el lado de la empresa, honestamente, me da mucho miedo.

¿Qué es lo que está pasando? En un artículo se establece que la autoridad va a definir, en función del estado de la tecnología, los requisitos y condiciones de seguridad que deban de mantenerse en las empresas.

¿Qué es lo que me inquieta? La tecnología se modifica y va creciendo y va actualizándose constantemente.

Si como empresa voy a tener que estar comprando equipos en función de los requerimientos o de lo que se le ocurra a la autoridad, la verdad es que para mí implicaría un cheque en blanco. O sea, vamos a ver qué me dice la autoridad, o si voy a tener que comprar el último programa de software o el equipo más grandote, pues imagínense nada más en el ámbito de empresa mediana y pequeña.

La verdad es que supone una cierta incertidumbre por seguridad. Mejor habría que hablar de gestiones razonables o cuestiones en eses contexto.

Otra cuestión interesante es el caso de la autoridad encargada. En ese entonces, 2001, se hacía referencia en específico a aquélla que dispusiera la Ley Federal de Transparencia y Acceso a la Información Pública.

Y yo me pregunto aquí: Bueno, el IFAI para todos los casos, también cuestiones públicas, cuestiones privadas. Originalmente la iniciativa del senador García Torres iba referida a la creación de un instituto *ad hoc*. Posteriormente, hubo por ahí en la propia Cámara de Senadores alguna adecuación para aprovechar la parte relativa a la que ya refería la Ley de Transparencia y Acceso a la Información Pública Gubernamental.

En este sentido y plantando el tema referido en específico a la autoridad encargada, pues yo quiero acotar que ya existen en la legislación vigente autoridades encargadas del cuidado, aplicación y sanción de conductas relacionadas con la protección de datos personales y de la publicidad con fundamento en disposiciones vigentes en México.

Tenemos, y ya habló Carlos Arce por aquí, la PROFECO, bueno Rafael nos acaba de comentar de CONDUSEF, el caso de CONAMET o el propio IFAI para el sector público, entre otras que ya existen.

¿No les resulta lógico que la autoridad en esta materia sea precisamente la que tiene el know how (saber cómo o saber hacer), la reguladora del marco de la actividad de la persona u objeto

de la empresa en específico que en su momento pudiera recabar la información?

¿Qué nos puede garantizar en este sentido? De alguna manera eficiencia operativa y un menor costo al erario público, no sin descuidar, y esto es algo importante porque ya Carlos Alonso lo refería en su exposición, el esquema de autorregulación de las empresas manejando esquemas relativos a avisos de privacidad o cuestiones relativas a áreas de actividad en específico.

Me queda claro y nos queda claro, yo creo necesaria la creación de una Ley Federal de Protección de Datos Personales, en mucho se tiene que hacer, pero también nos queda claro que tenemos regulaciones específicas y muy concretas, dependiendo de diferentes actividades.

Entonces pues podría resultar razonable el hecho de manejar no una autoridad única encargada de la materia.

Moderadora: Isabel Davara Fernández de Marcos. Consultora especialista en Protección de datos personales.

Yo coincido, no sé si estancamiento es la palabra de la legislación en protección de datos en México, porque con tantas reformas e iniciativas contrapuestas que se conocen, pero el hecho de que desde hace más de cuatro años no haya salido una iniciativa o una ley ya preocupan.

Creo que, como decía el doctor, el sano equilibrio es el *kit* de esta cuestión. Como me ha puesto la bandeja tengo que contestar; en cuanto a lo del Tratado de Libre Comercio con América del Norte, si en América del Norte estamos considerando a Canadá, Estados Unidos y México, y Canadá tiene una legislación que cumple con la europea y Estados Unidos es una estación en el mundo mundial, pues México puede tener una legislación que cumpla con la europea y así también cumplir con Estados Unidos. Quiero decir, podría llegar a una solución de consenso, no tanto seguir con la tradición estadounidense, sino seguir con la tradición canadiense que, digo, es la que sigue el resto del mundo que está legislando en protección de datos y así salvar el Tratado de Libre Comercio con Estados Unidos y el Tratado de Libre Comercio con Europa.

En cuanto a los archivos. Es que tu pregunta es muy buena, porque esto ya sería más técnico, pero cuando decías si una "kueri" o no una "kueri", estamos entonces viendo que va a haber un tratamiento de información posterior y específico.

Aquí habría que distinguir entre un archivo físico, un archivo lógico y un archivo jurídico. A nosotros el que nos interesa es el jurídico que se califica por los datos que contiene, pero, sobre todo, por la finalidad a la que se destinan esos datos.

Y esos archivos que mencionabas, probablemente en mi opinión serían temporales, que no entrarían dentro de un sistema de registro como tú decías.

Haz mencionado también un tema clave en todas estas normas de tecnologías de información y comunicaciones. La norma tiene que ser necesariamente neutral desde un punto de vista tecnológico, no me pueden decir qué tecnología tengo que implementar, si no lo que tengo que conseguir, por dos razones muy claras.

Una razón de obsolescencia y otra razón de competencia en el mercado. No me van a decir utiliza esa máquina o ese Software.

Y en cuanto a las diversas autoridades, yo ahí discrepo, sé que está dividido, yo creo que esta es una cuestión como para que hubiera una autoridad central encargada de la materia.

Pero por eso mismo, como todas ellas tienen un pedacito de ámbito de competencia, se van a empezar a: esto es mío, esto no es mío. De repente hay una en la que dos tienen competencia y hay una en la que nadie, hay una laguna.

La protección del personal es una materia que por sus características va a permear todos los ámbitos y todas las materias de la sociedad, no va haber ninguna cuestión en la sociedad que no se vea permeabilizada, por lo cual, mi opinión es que debería de haber una autoridad de control que diera cuenta de estas materias.

Sin más pasamos a las preguntas, hay miles. No sé quién quiera empezar. Nos han ido pasando preguntas.

Ponente: Rafael del Villar Alrich.

¿Qué normas regulan los *Burós de Crédito* y las Sociedades de Información Crediticia? ¿Quién administra y controla los *Burós de Crédito*? ¿Cuáles son los requisitos para establecer un *Buró* de Crédito independiente? ¿La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental es el conducto para pedir información de operaciones crediticias propias, dónde se es parte, o mejor usar exclusivamente la legislación especializada? ¿El IFAI es autoridad para ordenar, entregar versiones públicas de operaciones crediticias? ¿Proceden las versiones públicas de operaciones crediticias?

Las normas que regulan al *Buró* de Crédito. La ley, es una ley emitida a principios del año 2002, reformada a principios del 2004. La ley se llama Ley para Regular las Sociedades de Información Crediticia, y en ésta se establecen derechos del consumidor, estas garantías de protección de la seguridad de la información, y también establece y regula con toda claridad el proceso de autorización para nuevas Sociedades de Información Crediticia. También contiene un capítulo de sanciones, en fin.

Es una ley, que podríamos decir que es una ley completa para la regulación de estas empresas cuyo ámbito de acción, y eso sí es importante mencionarlo es exclusivamente el de reportes de historiales crediticios. Ese es, digamos, el ámbito de esta ley.

Banco de México, de acuerdo con esta ley tiene diversas atribuciones regulatorias, y ha emitido unas reglas que se llaman *Reglas generales a la que deberán sujetarse las operaciones y actividades de las Sociedades de Información Crediticia y sus usuarios*.

Los usuarios de esta ley son precisamente a los que yo me refería como oferentes de crédito. Son los clientes de esas Sociedades de Información Crediticias, son precisamente los otorgantes de crédito.

Estas reglas emitidas por Banco de México regulan, entre otras cuestiones los detalles, garantizan el derecho de acceso a los reportes de crédito especiales de las personas a tarifas reguladas.

Y también establece con claridad los casos en que se puede sustituir, digamos, el caso de excepción a la regla general que es la firma autógrafa. ¿Cuándo se puede sustituir la firma autógrafa? Como ya lo mencione en estos casos en que los *Burós de Crédito* coadyuvan, apoyan a actividades de mercadotecnia directa. Hay forma de sustituir la firma autógrafa con un proceso de identificación de la persona.

El proceso de identificación de la persona también es muy importante, es clave para el acceso eficiente a los reportes de crédito especiales, porque uno llega a la página del *Buró de Crédito*, y ahí en esa página, lo que uno hace ir llenando un cuestionario que tiene que estar bien llenado, incluyendo información de créditos otorgados para estar seguros de que se está identificando esta persona. Entonces estas son las reglas.

¿Quién administra y controla los *Burós de Crédito*? Son entidades privadas, son empresas privadas. Tienen las reglas de operación, se rigen bajo las leyes mercantiles, como tal; además de la Ley para Regular las Sociedades de Información Crediticia.

¿Cuáles son los requisitos para establecer un *Buró* de Crédito independiente?

Bueno, es muy simple la idea, la idea de un *buró* independiente estábamos refiriéndola a la independencia de los oferentes de crédito. Es decir, digamos que era un modelo o un esquema distinto del modelo de club.

Entonces, donde son un grupo de oferentes de crédito que forman su propio *Buró de Crédito*, un *buró* independiente sería un *buró* que no tiene vínculos patrimoniales o de control con oferentes de crédito o estos vínculos son pequeños.

En cuanto a una pregunta que dirigen tanto a mí como a mi tocayo Rafael Avante Juárez, pero que yo creo que debería de estar dirigida al Comisionado Juan Pablo Guerrero, perdón, es en relación a la Ley Federal de Transparencia y Acceso a la Información, de si el IFAI es autoridad para ordenar entregar versiones públicas de operaciones crediticias.

No, digamos, el no es que no soy la persona que deba de contestar esta pregunta. Del secreto financiero, es un secreto que está interpretado y regulado por las autoridades financieras y eso está muy claro.

Difícilmente sin el consentimiento de la persona, por eso hablamos de asista a la Ley para Regular las Sociedades de Información Crediticia, difícilmente sin el consentimiento de la persona a la que se refieren los datos crediticios, esta información puede fluir a un tercero.

Existen excepciones, como todo, cuando lo ordena un juez, cuando es parte de un proceso de concesionamiento de autorizaciones, como ya comentaba también Juan Pablo Guerrero.

Pero la regla general es: El acceso a esta información de parte de las autoridades, es básicamente hacia la Comisión Bancaria y de valores, que es el regulador, el supervisor de estas leyes.

Ponente: Juan Pablo Guerrero.

Nuestra moderadora provocadora nos hizo varias preguntas, muchas veces muy buenas.

Y yo quiero atender a uno de tus planteamientos, Isabel, sobre la propuesta de que la publicidad puede mermar la privacidad.

Estamos de acuerdo en que hay un conflicto de principios, supongo. Y lo que hemos intentado es enfatizar en aquellas resoluciones en donde obligamos a dar información que fue clasificada como confidencial, obligar a dar la información que revele la actuación de la autoridad y su relación con las personas, respetando lo más posible la información personal. Allí es donde hemos ido trazando este equilibrio.

Pero de que hay un conflicto no tenemos duda, cada vez más tenemos precisamente este tipo de quejas que nos obligan a hacer este tipo de ponderaciones.

Y un apunte con relación a lo de los créditos. Efectivamente, cuando el sujeto obligado es un banco de desarrollo, es decir, banca pública, banca del Estado, el IFAI ha confirmado que por el secreto bancario no puede dar la información.

Hay dos consideraciones sobre el particular. Una es cuando el acreditado es otro sujeto obligado, lo que hemos procedido a hacer es orientar la solicitud al acreditado, no estoy hablando ya de personas, y en principio no tiene por qué invocar el secreto bancario y es el que legalmente, con absoluta confianza con la Ley de Instituciones de Crédito, tiene la autorización de darle información sobre su crédito.

Y la otra excepción es cuando el acreditado es un empleado de alguna de las bancas de desarrollo, ahí hemos asumido el crédito como una prestación y no hemos diferenciado que sea un empleado de Bancomex, de Nafinsa o del IFAI que ocasionalmente también podría darle un crédito a sus empleados como algún tipo de prestación.

Me quiero referir a un par de preguntas y les voy a pedir a aquellos que no sientan que atendí a su pregunta, que me vengan a ver al término de esta sesión, si no porque muchas de sus preguntas se refieren claramente a el Instituto y mi labor ahí como Comisionado y no tanto a nuestro tema de esta sesión.

Esta sí está claramente vinculada, ¿qué va a pasar con los lineamientos que emitió el IFAI en materia de datos personales cuando se apruebe la ley en la materia? Habrá que ver el contenido de esa ley si se sigue planteando una distinción entre las bases de datos en posesión de los sujetos obligados por la Ley de Transparencia, es decir por el sector público y el sector privado.

El IFAI seguirá siendo la autoridad en la protección y acceso a las personas a sus datos. Todo indica que es posible que esto no sea así, que la Ley de Datos Personales incluya también a los datos en posesión de entidades públicas, con lo cual se tendría que hacer la adecuación correspondiente, dado que quedaría subsumida esta regulación en la nueva ley.

Lo cierto es que entre tanto, como bien nos decía Alfredo, hoy en lo que se refiere a las bases de datos en posesión del Estado mexicano, se tiene ya la regulación correspondiente.

Hay otra pregunta con relación a las empresas de *marketing* y la utilización de datos personales para fines comerciales. En el caso de las entidades y dependencias públicas no hay ninguna disposición que permita su comercialización y los propios lineamientos a los que se hacía referencia en la primera pregunta escrita, establecen que si se diera alguna condición específica, tendría que ser con el consentimiento expreso del titular de esos datos.

Quiero subrayar que estamos hablando de algo que hoy por hoy no existe; ni Pemex ni CFE ni el SAT, imagínense ustedes, puede comercializar con sus bases de datos e institucionalmente la posición del Instituto es que esto así debiera ser, dada la razón por la cual el Estado obtiene datos personales de las personas, que es muy distinta, ahí las personas están obligadas a dar información sobre sí mismas, es muy distinta a la regulación del sector privado.

El IFAI es competente para ordenar la apertura de la información bancaria, cuyos titulares sean los sujetos obligados, siempre y cuando sea el cuentahabiente el sujeto obligado.

Si ustedes quieren saber cuánto dinero tiene en su cuenta el IFAI, pregúnteselo al IFAI, no se lo pregunten a HSBC, no se los va a dar HSBC, porque si lo hiciera violaría el secreto bancario y entre otros, el IFAI los demandaría.

Ponente: Hugh G. Stevenson. Director Asociado, Comisión Federal de Comercio EE.UU.

¿La venta, renta o el compartir las listas de clientes entre empresas privadas, está prohibida en los Estados Unidos? Sí, ¿por qué? Si no, ¿cuál es la tendencia a futuro?

Y creo que la respuesta es que estamos enfocados en dónde está la posibilidad de daño, dónde están ahí los problemas en sí, por lo general no está prohibida.

La ley prohíbe el compartir estos documentos en muchas situaciones, ¿por qué? Porque en estas dos situaciones hay la posibilidad de daño, es información muy sensible, muy asociada con el robo de identidad de que hemos hablado.

Hay también otra posibilidad de daño, al bienestar de los consumidores o usuarios. Es si se introducen en la intimidad, por ejemplo, con Spam o con las ofertas de crédito.

Había también una pregunta sobre la autorregulación y la comparación entre los Estados Unidos y la Unión Europea. Y algo interesante a pensar en cuanto a eso es más que sólo las reglas, es también la cultura y la autorregulación.

Un ejemplo para mí, que me parece muy interesante. Es que hace algunos años Consumer International ha escrito un informe sobre las políticas de privacidad en la red y ha encontrado que en general había más políticas por las empresas en los Estados Unidos, donde no debía haberlas, que en varios países en Europa donde sí debía hacerlo.

Ponente: Rafael Avante Juárez.

En cuanto al planteamiento de Isabel, partir de que coincido totalmente, hay que partir de un punto de equilibrio, no podemos cargarnos a ninguno de los dos lados de la balanza.

Me decías que es fácil ponerse de lado del usuario, vieras a veces que es un poquito complicado llevar el punto de vista del usuario a la toma de decisiones, pero sí efectivamente es la parte noble del tema.

Y que hay usuarios tramposos. Sí, aunque yo te diría que en mi experiencia son los menos y que sería una desmesura generalizar para poner medidas contra los tramposos a todos.

El estado de la cuestión: iniciativa de Ley Federal de Protección de Datos Personales

Mesa 6:

Moderador: Alonso Lujambio Irazábal. Consejero del IFAI.

Vamos a ser testigos de un banquete sobre el debate mexicano.

Creo que no es un rasgo de parroquianismo ni de localismo de los organizadores del evento el establecer esta mesa.

Estoy cierto de que el caso mexicano, el proceso legislativo en curso es expresión exquisita a mi juicio de la complejidad del debate sobre la protección de los datos personales, tanto del debate doméstico como del debate internacional.

Hago una brevísima reflexión sobre esto para iniciar, si me lo permiten, la discusión en la mesa.

Respecto a la dimensión doméstica es indudable que ciertamente no hay una cultura de protección de datos personales en México y en América Latina.

Y, sin embargo, creo que un debate central en relación con este punto es y voy a citar a uno de nuestros amigos en una mesa previa, darle a la ley la oportunidad de crear la cultura. Creo que es parte de nuestro debate.

Por otro lado, hay una realidad que nadie puede negar, ya hay una circulación amplísima sin control de datos personales y estamos ante el debate, lo hemos subrayado una y otra vez, pero qué bueno que así sea, ante el dilema del equilibro entre dos valores en tensión, la protección de datos personales, la protección de la privacidad de las personas y, por otro lado, la legítima transmisión de datos para efectos de eficacia del mercado de crecimiento económico.

¿Bajo qué condiciones puede darse este equilibrio? Se habla del consentimiento expreso y previo en algunos casos, de la oposición expresa y posterior en otros.

Yo ciertamente me he inclinado ligeramente hacia la visión garantista, pero reconozco y mis colegas comisionados del IFAI también, que el gran reto es encontrar ese equilibrio entre la visión mercantil y la garantista.

Estamos ante un reto extraordinario político, legislativo, técnico, logístico.

Está, por otro lado, amigos, la dimensión internacional, en donde se expresa ciertamente esa tensión. Tenemos compromisos con la Unión Europea, con la APEC, con nuestros socios comerciales del Tratado de Libre Comercio.

La convergencia en nuestro marco legal de esos compromisos, no siempre compatibles de modo automático, mecánico, es sin duda un reto mayúsculo para el legislador mexicano.

Está, por otro lado, y cierro esta reflexión con este punto, el debate sobre la autoridad, debe ser el IFAI en el caso mexicano o debe ser otra autoridad.

Creo que en primer lugar la obligación del IFAI aquí es contribuir constructivamente al debate, creo que es su obligación es además su vocación.

¿Por qué creo y por qué creemos los comisionados que esta es la institución que debe de enfrentar el dilema regulatorio y la responsabilidad cabal? En primer lugar, porque reduce los costos de administración de nuestras instituciones, pero especialmente porque tiene un capital de prestigio social y político para emprender la tarea.

Y esto lo digo, quizás, el Comisionado sea el único que lo puede decir, porque ese capital de prestigio social y político ha sido producto de mis colegas, del trabajo de mis colegas comisionados y de los funcionarios de la institución.

Porque, por otro lado, ha probado su independencia, que es un criterio fundamental para realizar esta función; porque tiene el personal especializado, indudablemente; porque reconoce la necesidad de armonizar lo valores de intención mencionados y no está casado con uno de los dos extremos del debate.

Porque coorganizamos este Encuentro de Protección de Datos Personales; porque somos parte de una Red Iberoamericana; porque somos ya autoridad en la materia, así sea restringida, y porque el tema nos preocupa, nos ocupa cotidianamente, nos importa.

Con todo, respetaremos cabalmente, amigos legisladores, insisto, a cabalidad la decisión que tome el legislativo, que sin duda será la mejor para el país.

Estamos ante un debate muy interesante y yo debo finalizar esta reflexión diciendo que la realidad se está moviendo todo el tiempo y no deja de moverse.

Yo creo que hay un espacio para la creatividad mexicana, no solamente para acomodarse a la situación nacional, sino para crear una situación a la que otros se acomoden.

Me llama mucho la atención, y con eso cierro, que el día de hoy el Washington Post publique una noticia que me parece de la más alta relevancia: El anuncio que hace Microsoft en Estados Unidos, de difusión de una National Privacy Law, una nueva ley de privacidad, que tienda a ser mucho más proteccionistas y mucho más garantista que lo que hoy tiene el marco norteamericano.

Y debo leerles la nota de hoy que dice, entre otras cosas, "que la propuesta de Microsoft es que exista la opción del *opt-in*, es decir, la opción el consentimiento expreso y previo, para los datos sensitivos, "y que apoya la opción *opt-out*, es decir, la oposición expresa y posterior, para los datos de menor sensibilidad.

Y termina diciendo: "Sin embargo, el diablo está en los detalles". Es indudable que el diablo está en los detalles y que, sin embargo, por fortuna, aun con la complejidad del trabajo, los legisladores mexicanos y muy especialmente el senador García Torres, que esta sentado a mi izquierda, ha sido indudablemente el mexicano que de manera más decidida ha aportado a esta importante discusión.

Le debemos mucho al senador y le debemos mucho que esté entre nosotros, al igual que el resto de los legisladores de esta mesa.

Voy a presentar a Francisco Javier Acuña Llamas, quien es integrante del Sistema Nacional de Investigadores del CONACYT; Coordinador del doctorado en Derecho en la Universidad Anáhuac del Sur. Es profesor especialista en Derecho de la División de Derecho de Postgrado de la UNAM; es profesor e investigador del Instituto de Investigaciones Jurídicas de la UNAM de 2003 a 2004. Es doctor en Ciencias Políticas y Sociología, por la Universidad Complutense de Madrid.

Es licenciado en Derecho en la Facultad de Ciencias Jurídicas de la Universidad Regiomontana, A.C. de Monterrey, Nuevo León.

Conferencia Magistral: Francisco Javier Acuña Llamas.

Agradezco venir a externar algunas palabras en relación a la iniciativa que planteara, con mucha preocupación, el senador García Torres.

Debo decir que estar aquí, frente al senador y junto con todos ustedes, es un compromiso de agradecimiento a él, por haber provocado naturalmente, con esa iniciativa, una cauda de reacciones de muy interesante entidad, de toda índole; las primeras, algunas, hasta bruscas o fuertes, en relación a lo que se pudo haber comentado o se comentó, que pudo haber sido aquello una adopción de un modelo garantista extremo, el que se parece mucho, el que la iniciativa invocaba la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, Lortard española que fue, incluso, abrogada en el año del 99. Es decir, la iniciativa de García Torres fue una iniciativa muy parecida a los principios y a los contenidos de aquella ley que tuvo España en aquellos momentos, y que dejó de tener vigencia porque hubo directivas de la Comunidad Europea que impidieron se mantuviera vigente y hubo allá que hacer nacer una nueva ley, la ley vigente.

Sin embargo, la provocación del senador García Torres ha venido a mantener en jaque todo este tiempo, y eso es lo saludable, además del tema. La necesidad que en México se tiene de dar el paso definitivo para crear, para construir una legislación pertinente.

Una legislación que resuelva ese dilema que desde un principio vimos y tenemos en México. Se optó en México por darle el sí al acceso a la información pública, y se optó también, hay que decirlo, por los actores políticos, los legisladores, sobre todo, decidieron darle el sí al acceso a la información pública, y decidieron, de alguna manera, también permanecer, cautelosos en cuanto a darle el sí paralelo a la protección omnicomprensiva de los datos de carácter personal.

Desde luego las leyes de acceso a la información pública, empezando por la federal, contemplan su capítulo respectivo de previsiones para fomentar y para proteger el acceso a la información de los ciudadanos respecto de sus propios datos.

Y en esto las estadísticas no reflejan, el propio IFAI las difunde que del cien por ciento de las solicitudes de acceso a la información que éste ha recibido, muy escaso el 10 por ciento, que es mucho menos que el 10 por ciento, algo menos que el 10 por ciento ha versado sobre solicitudes en relación a los datos de carácter personal.

Ya decía el Comisionado Lujambio si en México todavía el tema del acceso a la información pública causa, en algunos lugares y en algunos niveles perplejidades, más lo causa, desde luego, el tema de estrenar el derecho a reclamar el conocimiento de aquellos datos que tiene el Estado sobre nosotros mismos.

Si bien históricamente el moderno Leviatán, la administración pública, el Estado ha sido el detentador y es el detentador de una muy importante partida de datos personales que todos los ciudadanos le entregamos todos los días en esa alcabala sucesiva permanente, en la que con cada trámite de dejamos, le damos, le

entregamos datos personales que almacena, a veces, de manera riesgosa, porque no los sabe guardar bien, a veces simple y sencillamente almacenados hasta el futuro o sea a perpetua, porque no hay regulación precisa que lo impida.

El hecho es que hoy por hoy y en el mundo contemporáneo no es el Estado, a pesar de tener, ya lo dije, peligrosos mecanismos para si quisiera hacer mal uso de estos datos, causarle daño a la ciudadanía, sino es el propio mercado o es el ámbito del sector privado en el que se encuentran los más grandes peligros, para que el derecho al intimidad se pueda ver conculcado.

Y esto, porque debido a la tendencia, conocida como despublificación, mal llamada así, pero así conocida en España, sino más bien por los efectos del acto habilitante, mediante el cual el Estado confiere a particulares cada vez más grandes zonas de participación en prestación de servicios públicos y/o además los propios giros del mercado con todas las tecnologías de punta y los nuevos mecanismos de comunicación, realmente nos encontramos ante un hecho que es irrefutable, y que aquí se ha venido diciendo por todos los grandes expertos que han venido de todas las latitudes que convoca ese encuentro, y ahí es donde encontramos el principal peligro.

Hoy por hoy, y tras los antecedentes del *ChoicePoint*, aquel penosísimo antecedente en el cual fueron filtradas las bases de datos de toda la población que tenía derecho o que tenía edad de votar en el año del 99, tras ese experimento funesto del RENAVE, que quedó varado, pero que también significo un peligro potencial de filtración de datos personales confiados a un grupo de particulares en ese Registro Nacional de Vehículos que quedó también varado, que quedó también, afortunadamente, inutilizado y además de los hechos recientes de manipulación de padrones de usuarios de servicios públicos y, sobre todo, de padrones de beneficiarios de subvenciones o de cualquier otro tipo de subsidios que el Estado a través de los programas públicos hace llegar constantemente a la ciudadanía.

Pero ojo, para fines electorales, el caso de Tlaxcala concretamente, pero otros más casos nos pone a todos en la necesidad de invocar en esta mesa y de agradecer al IFAI que una vez que ha dado cauce al tema del acceso a la información y que ha logrado desde luego en esto grandes avances, haya tenido el ánimo de encausar esta mesa de discusión y de invitar aquí al senador García Torres y a otros senadores y a otros legisladores para impulsar definitivamente una ley.

Nosotros, en síntesis, venimos a terciar en una discusión que dice, por el lado de las empresas de mercadotecnia directa, que como ya hay regulaciones parciales sobre derechos de autor, sobre el consumidor y sobre las sociedades de la información crediticia, pues que ya se queden las cosas así y que de esa manera ya está resuelto el problema.

De ninguna manera, creemos que urge una regulación integral, siempre hemos sostenido que debe ser o debiera ser una ley general la que regulara el tema de los datos de carácter personal para que fuera una regulación transversal que abarcara todos los estados, a las entidades federadas todas, por supuesto, salvo Colima que es la que ya reguló en el ámbito propio en su localidad el tema de los datos de carácter personal de manera amplia; en todos los demás casos tenemos el mismo pendiente.

Dicen algunos que esto implicaría que algunas leyes se derogaran, pues ni mido. Sí, desde luego una ley general vendría a derogar muchas disposiciones aisladas al respecto, pero ese no es el problema, el problema es resolver la gran situación de desregulación que tenemos como ya lo avisábamos y lo venimos mencionando.

De verdad me alegra escuchar la nota que nos leía el Comisionado Lujambio sobre la posición de Microsoft que se rebelaba ya, en la que ellos aceptan algunas de las posiciones de Opt-in, o cual es saludable del todo y habla que acaso este congreso venga a darle sintonía a una postura más flexible de los grupos de mercadotecnia directa, que junto con Microsoft están en una

posición que urge colocar al equilibrio, como ya lo decía la Comisionada María Marván al principio de este Encuentro, para que un equilibrio, una visión equilibrada venga a resolver el problema.

Si no pudiera haber una ley general, pues urge entonces una ley federal que atañe al ámbito federal del Estado y sigue dejando en el ámbito de los estados de la Federación que resuelvan ellos poco a poco y paso a paso como ha sido materia de acceso a la información pública y de transparencia el asunto. Y en eso hemos visto lo disparejo y lo distante que pueden ser las posiciones en nuestro vasto escenario nacional.

Por eso en una cuestión tan delicada, como es una cuestión del derecho fundamental a la intimidad, el derecho al honor y el derecho a la propia imagen que tiene muchas formas de expresión en la variada manera en la que los ciudadanos hacemos valer nuestro derecho a la privacidad en estos tiempos agitados y modernos, nos parece que de debe ser una ley general.

Para acabar, si el IFAI o no el IFAI, por supuesto que el IFAI debiera ser el órgano garante, pero eso sí tendría que antes verse la cuestión de la transformación del Instituto Federal de Acceso a la Información Pública en una entidad que tuviese un rango distinto al que ahora tiene, porque si bien es un órgano, una autoridad independiente que lo ha sido en los hechos y nada de duda cabe en ello, si bien es cierto es una cuestión, no es una posición virginal, de verdad lo digo, pero está todavía incrustado y limitado al ámbito de la administración pública que dirige el Presidente de la República en su carácter de Jefe de gobierno y por esa razón solamente le toca o es el órgano garante de la transparencia y el acceso a la información pública y de la protección de los datos personales, pero dentro del ámbito de la Administración Pública Federal.

Esto para los que no están familiarizados con la realidad nacional, pues solamente es el órgano garante de la transparencia dentro del Poder Ejecutivo Federal y no abarca a los otros poderes públicos ni por supuesto a los órganos constitucionales autónomos.

Entonces, pues, así las cosas, pediríamos que el Encuentro arroje luz y que los señores legisladores ya que han detenido esa iniciativa, que fue incluso aprobada la del senador García Torres y por unanimidad en el Senado, ahora que está en la Cámara de Diputados pendiente de resolución, se aproveche para que con la confluencia de una posición más elástica que ya se advierte de los grupos de mercadotecnia directa, que es la que nos está avisando ya esta nota que se publicara en este influyente diario norteamericano, permitiera replantear las cosas, y esto se sumara, quizá, a la contribución generosa de entender que el IFAI pudiera alcanzar la categoría de un órgano constitucional autónomo, que tuviera esa doble vertiente.

Es decir, lo que de suyo ya tiene ahora, pero para el puro Ejecutivo Federal, pero ahora extensiva a todos los ámbitos del nivel de la Federación y además, que pudiera incluir abrazar la regulación de los bancos de datos de carácter privado, que de otra manera no habría manera de ponerlo o de convertirlo en autoridad suficiente o capaz de tutelar el *Hábeas data* institucional que podría o que se está proponiendo.

Esto al margen de que se regule también y como ya la propia iniciativa García Torres lo menciona, pero en este caso a nivel de la justicia federal y de la justicia de los estados procedimientos ágiles, sumarios de *Hábeas data*, para que en caso de que no sea suficiente la suerte que tenga el ciudadano que se ve obstaculizado de conocer sus datos, los datos de los cuales es titular a nivel de las dependencias burocráticas y que incluso el remedio que hubiese ante el órgano garante le fuera adverso, pudiera ir como de hecho lo puede hacer, pero mediante un procedimiento sumario, sumarísimo, que le hiciera no vivir una aventura desastrosa que luego lo invitara a no volver a repetirla en el futuro.

El asunto en este caso está en reflexionar agudamente en la necesidad de considerar que el IFAI así como está, me parece, no podría adquirir la categoría o la cualidad, la calidad de ser autoridad para extender sus potencias al ámbito privado como regulador.

Me parece que necesitaríamos pensar en la oportunidad histórica que el IFAI encontraría para convertirse en un verdadero organismo constitucional autónomo que regulara el acceso a la información pública, la transparencia y además, de manera omnicomprensiva los datos de carácter personal, que ya dije, no sólo están siempre en riesgo, siempre, humanamente en riesgo en el ámbito del sector público, pero, sobre todo, en el ámbito del sector privado; hoy por hoy los *Burós de Crédito* son sin duda alguna el latiguillo o el verduguillo que más está generando situaciones de discriminación que por la vía de la cuestión laboral ha venido ha generar enormes situaciones de lamentar sin para las que haya hasta ahora verdaderos remedios que ofrecer.

Por esa razón pedimos que la normativa se vigorice, que las posiciones se elasticen, que nos acerquemos todos a un punto intermedio, que aprovechemos de la iniciativa de García Torres el impulso, el empuje, algunos de los mecanismos que ya adelanta opt-in que tomemos de las propuestas de Banco de México y del sector, sobre todo, de las empresas de mercadotecnia directa las propuestas de opt-out que son más abiertas, más vigorosas, porque indudablemente, con esto cierro, el mercado y el Estado se alimenta de datos personales, nadie lo puede negar, el Estado y el mercado tienen como combustible permanente los datos personales de usuarios, de clientes, de noticiarios, etcétera.

Lo que urge es que se protejan los datos personales sensibles, como ya se reconocía también, de manera externa, pero los datos personales de carácter comercial pueden tener precio, pueden ser vendidos y deben circular incesantemente porque esto es lo que en el mundo moderno existe, y México en este caso ya vinculado con Europa a través de ese Tratado de Libre Comercio y vinculado también con los Estados Unidos y el Canadá y con muchos hermanos de América Latina no puede quedar al margen de una regulación satisfactoria que como el caso de Argentina esté ya certificada con ese beneficio de ser confiable para las transacciones y para los flujos transfronterizos que exige la realidad económica mundial.

Moderador: Alonso Lujambio Irazábal. Comisionado del IFAI.

Le voy a dar la palabra a nuestro amigo el senador don Antonio García Torres, es licenciado en Derecho por la Universidad Nacional Autónoma de México; Secretario de Gobierno del Estado de Michoacán, Magistrado del Tribunal Superior de Justicia del Distrito Federal, Subprocurador de la República, entre otros cargos públicos. Ha sido profesor de la Facultad de Derecho de la Universidad Autónoma del Estado de Hidalgo.

Actualmente es Senador de la República, Presidente de la Comisión de Estudios Legislativos, una comisión estratégica por la que pasa prácticamente toda la producción senatorial. Presidente del Comité de Transparencia y Acceso a la Información Pública Gubernamental del Senado de la República, también de la Comisión. Integrante de la Comisión Bicameral en materia se Seguridad Nacional del Senado de la República.

Es promovente, ya lo he dicho, lo sabemos todos, de la Ley de Seguridad Nacional hoy vigente y también, por supuesto, iniciador de la Ley Federal de Protección de Datos Personales.

Ponente: Antonio García Torres.

Primeramente quisiera agradecer a la Comisionada Presidenta del IFAI, la invitación para participar con ustedes esta tarde, en este foro tan importante para lo temas que nos ocupan.

Y, en segundo lugar, también quisiera hacer un reconocimiento al doctor José Luis Piñar, Director de la Agencia Española de Protección de Datos,

quien ha sido en realidad un gran impulsor de esta legislación en Iberoamérica, ha sido un consultor de toda la gente que estamos interesadas en el tema y ha auxiliado a muchos países en las redacciones de sus leyes sobre la protección de datos.

Yo quisiera comentar con ustedes, porque nos lo han estado preguntando en los días de esta semana, que por qué queremos en México una Ley de Protección de Datos.

Ante la transmisión que existe hoy en día de datos con las tecnologías modernas, las carreteras de la informática y la facilidad para comunicarnos con el mundo entero, México se encuentra rezagado 35 años en materia de legislación de datos personales.

Esta legislación surge por primera vez en Alemania en 1970 y de allí empieza a irse extendiendo por todo el mundo, pasa a Francia, pasa a España, pasa a los Estados Unidos, pasa a países de América, como Argentina, como el Perú y como muchos otros países.

En febrero de 2001 yo presenté al Congreso una iniciativa denominada Ley Federal de Protección de Datos Personales. Esta iniciativa fue aprobada en abril de 2002, como se dijo aquí hace un momento, por unanimidad en el Senado de la República.

Yo quisiera aquí recordar con ustedes, que cuando se aprueba la Ley de Transparencia y Acceso a la Información Gubernamental, estaban las dos leyes corriendo los trámites legislativos y entonces se dio un trabajo parlamentario para poder avanzar y fue así como nos pusimos de acuerdo para que las dos leyes fueran aprobadas.

Lo que ocurrió fue que la Ley de Transparencia, cuando nosotros la aprobamos en el Senado, ya venía aprobada por la Cámara de Diputados y de inmediato se envió al Ejecutivo, para los efectos de la promulgación y publicación y entró en vigor.

Quiero señalarles que en el mes de diciembre de ese mismo 2001, fue cuando el Ejecutivo de este país presentó la Iniciativa sobre la Ley de Transparencia y Acceso a la Información Pública Gubernamental. O sea, se presentó muchos meses antes la Ley de Protección de Datos Personales.

Sin embargo, lamentablemente, después de que fue aprobada por el Senado de la República y enviada a la Cámara de Diputados, allí ha estado detenida de 2001 a 2005; han pasado ya cuatro años y las cosas han ido cambiando.

En el proyecto original de la iniciativa presentada por mí se establecía un Instituto de Protección de Datos Personales, como el órgano de control de la aplicación de esta ley.

En esa negociación que hicimos con los otros partidos políticos, tuvimos que quitar el Instituto ya de la minuta aprobada por los senadores, como también tuvimos que quitar la protección de las personas morales que también estaba establecida en el proyecto original, y le hicimos varios cambios, en un afán de avanzar y de ver cómo caminarían estas nuevas instituciones en nuestro país.

Después de tres años de que el IFAI ha venido trabajando y que ha surgido cada vez más la necesidad de controlar los datos en términos generales, porque la transmisión de éstos es inmensa. Yo les podría comentar que aproximadamente el año pasado de nuestro vecino país, los Estados Unidos a México, se transmitieron 50 millones de datos. Eso nos da una idea de la magnitud de este tema, de este trabajo, y que hoy en día en México no existe ninguna regulación.

No tenemos regulación para los datos personales. Seguramente ustedes recordarán aquel gran escándalo que se presentó en México, cuando nos dimos cuenta que el banco de datos del IFE estaba en una agencia de los Estados Unidos, que había sido adquirida, comprada en México, y también el banco de datos de licencias de la Ciudad de México.

Los bancos más grandes quizás que pueda haber, yo de los que conozco es el del Seguro Social, que tiene más de 55 millones de datos de personas, y después el de nuestro padrón electoral, que cuando se dio a la venta tenía más de 50 millones, y para el año próximo, que tendremos un proceso electoral, está arriba de los 70 millones.

Todas estas cuestiones fueron las que nos impulsaron a nosotros para presentar esta iniciativa. El estado actual, como les he manifestado se encuentra en la Cámara de Diputados, y aquí nos acompaña el diputado David Hernández, quien es Secretario de la Comisión de Gobernación, que es una de las comisiones que van a dictaminar esta iniciativa, y que aquí en cortito yo le decía hace un momento: Oye, diputado, ¡ojalá! que logremos sacar esta ley en este periodo, para ya asignarle presupuesto, y que pueda realmente el año que entra empezar a entrar en vigor y a ver de qué manera llegamos a los consensos, si no a los consensos, que es muy difícil, porque el consenso significa la voluntad del todo, y en la vida política de nuestro país actualmente sabemos que las fuerzas políticas representadas en el Congreso son varias, y que muchas veces es casi imposible llegar al consenso, pero sí podemos llegar a las mayorías.

De tal suerte que si lográramos que este tema sea deshogado en lo que nos queda de este periodo ordinario de sesiones, podríamos ya estar pensando en que para el año próximo tendríamos ya en vigor una Ley de Protección de Datos Personales, y que tendríamos, quizás, si así se decide por las mayorías, un Instituto que sea el órgano regulador de los datos personales.

La protección de datos personales es un tema que se había explorado en México muy poco, aunque se reconoce que existen algunos estudios que han sido realizados, sobre todo por la Universidad Nacional Autónoma de México, y se puede considerar que la discusión pública de este tema se suscita de una manera ya más fuerte a partir de la presentación de esta ley del suscrito.

La discusión se ha centrado de manera fundamental sobre los temas siguientes: Si los sujetos de protección han de ser sólo y necesariamente las personas físicas, o si también deben ser personas morales.

Si el objeto de regulación debe ser los datos que obren en archivos y bases públicas y/o privadas, bajo el entendido de que en estos últimos se pueden comprender los datos que por su naturaleza son de derecho social.

Si es aplicable el criterio del consentimiento previo a la recogida de los datos, cuando éstos no se colectan de fuentes de acceso público, este es uno de los temas que más ha influido en la discusión, si se necesita el consentimiento previo de la persona para poder transmitir y manejar sus datos personales, sobre todo, aquellos que van a su esfera más íntima, más cercana, como son sus derechos de la intimidad, del honor, sus tendencias religiosas, políticas, filosóficas, etcétera, o si se pueden transmitir y después obtener los consentimientos. Esta es una de las cosas más importantes que se están dando en el debate.

También si el flujo transfronterizo de datos requiere que los países en cuestión tengan niveles de protección equivalentes, si es necesaria una autoridad de control sobre los controladores de los datos personales, si el registro de las bases de datos personales es necesario, en todo caso, si cabe un remedio jurisdiccional para los conflictos que se susciten con motivo de la aplicación de la ley y cómo se puede lograr un equilibrio entre los objetivos económicos, el acceso a la información y la tutela de los derechos fundamentales a la intimidad, privacidad y autodeterminación informativa en materia de datos personales.

En el fondo lo que está en juego es si la Legislación mexicana se ha de inclinar por un modelo americano o por un modelo europeo para proteger los datos personales.

Hablar de un modelo americano o un modelo europeo no es enteramente correcto, dado que

en los Estados Unidos de América tan sólo por su régimen federal hay multiplicidad de formas de proteger los datos personales. Mientras que en Europa cada Estado ha adoptado formas muy disímiles a las de los Estados Unidos.

Sin embargo, en un intento por encontrar algunos referentes entre estas dos formas de proteger los datos personales, se podría decir que en los Estados Unidos de América existe una regulación legal parcelada, que hay una fuerte presencia de la autoridad judicial, que mucho también se deja a la autorregulación de los propios agentes interesados y que si bien se protege a la persona, es indudable el contenido económico de esa protección.

En Europa, por el contrario, la mayoría de los Estados europeos cuentan con una legislación general, con una presencia judicial no tan fuerte como en el caso americano y que se protege de manera primaria a las personas, sin que ello implique que se desatiendan los temas económicos.

El camino aparenta ser hacia un modelo mixto por la fuerte presencia de los intereses económicos y políticos de los Estados Unidos de América en México, por los crecientes intereses monetarios y generales de la Unión Europea y la necesidad imperiosa de proteger a la persona en un Estado que se perfila hacia una democracia cada vez más justa en un mundo globalizado.

En este sentido, parece que en México existe un consenso sobre la necesidad de una ley de este talento híbrido, el gran problema es el problema de la gran mayoría de las regulaciones se encuentra en el cómo, pues cada uno de los agentes involucrados persiguen que la legislación responda a sus particulares puntos de vista.

En ese cómo, los agentes privados que ahora controlan datos o que se perfilan hacia ese control, constituyen los grupos de interés más vigorosos, porque todos ellos se identifican entre sí, guardan intereses comunes y no es complejo que se pongan de acuerdo en torno a los puntos que estiman, quizá egoístamente, favorables o desfavorables de la regulación.

En este cómo proteger los datos personales, por otra parte, existen muchos ámbitos de interés: el financiero, el de la salud, los seguros, el laboral, la publicidad, entre otros.

En un esfuerzo por consolidad una opinión que permita transitar hacia la ley que proteja los datos personales, incluso los documentos de trabajo legislativos se han puesto a disposición de los interesados que se han acercado, paro paradójicamente no han revelado, cuando menos al suscrito, de manera expresa, sus posturas de frente a la regulación legal prevista en esos documentos de trabajos legislativos, como no sea el de la presencia de una idea de fuerza hacia la autorregulación.

Cualquiera que sea el derrotero de la iniciativa de la Ley Federal de Protección de Datos Personales, parece que podemos concluir en la necesidad de una regulación legal, con base en contenidos mínimos que se deben orientar, sí por las posturas de interés legítimo, pero también con sujeción a los instrumentos jurídicos constitucionales, a los instrumentos de derecho internacional y a la legislación secundaria que nos obliga.

Moderador: Alonso Lujambio Irazábal. Comisionado del IFAI.

María Eloisa Talavera Hernández, es egresada de la escuela de Ciencias de la Universidad Autónoma de Baja California, desarrolló el proyecto de Plan Municipal de Desarrollo 2001-2004 en Ensenada, fue regidora en el Ayuntamiento de Ensenada, fue Directora Administrativa de la Subprocuraduría General de Justicia del Estado en Ensenada, fue Secretaria General del Ayuntamiento de Ensenada.

Actualmente es diputada federal por el Partido Acción Nacional y Secretaria de la Comisión de Ciencia y Tecnología, miembro de la Comisión de Marina y miembro también de la Comisión de Economía.

Ponente: María Eloisa Talavera Hernández.

Yo iniciaría preguntando ¿Cuánto valen mis datos personales o cuál es el precio de la vida privada, que ese es el tema que está en discusión, frente a lo que son los derechos ciudadanos frente a la normalización de la legalidad informática y digital?

Y en ese sentido yo considero que la tecnología fue y sigue siendo el principal eje de la transición humana hacia la modernidad y el desarrollo y como tal los avances en este orden han sido siempre considerados como fuente natural para la emancipación de la humanidad y la conquista de las libertades individuales, pero al mismo tiempo dichos avances se han convertido una y otra vez en serias amenazas para la seguridad colectiva y personal de nuestras sociedades.

Con la emergencia y la consolidación de la llamada era de la información y el conocimiento y en los albores de este siglo, los avances tecnológicos han potenciado una vez más y a un nivel jamás visto en la historia, tanto en las promesas de libertad y desarrollo, como los peligros y las amenazas sobre la vida de los ciudadanos.

Y yo creo que a diferencia de otros momentos históricos la actual coyuntura tecnológica por lo menos en materia de informática no plantea una paradoja irresoluble, ni siquiera un peligro potencial de desintegración social, sino todo lo contrario, creo que hoy podemos aproximarnos al problema de la relación entre la sociedad y las tecnologías de información de una manera totalmente positiva.

Se lo debemos por supuesto a la madurez cívica alcanzada por las sociedades modernas, al avenimiento de un nuevo orden democrático frente a las viejas sociedades autoritarias y a la creciente participación ciudadana a través de movimientos sociales de nuevo tipo que valoran los principios de convivencia social y política.

Tenemos, entonces, una inmejorable oportunidad para construir un orden jurídico alrededor de las tecnologías de información que fortalezcan nuestras convicciones democráticas, nuestros principios humanistas y nuestras aspiraciones de equidad y justicia.

Quienes hoy promovemos las actuales reformas en materia de informática jurídica estamos obligados a responder cabalmente a esta oportunidades generando un marco legal a la altura de esta promisoria coyuntura.

Mi interés en esta presentación es plantear algunos de los retos que se nos presentan en esta materia, particularmente los que se refieren a la protección de los derechos de los ciudadanos en el marco de este proceso de maduración de la normatividad que deberá regir el funcionamiento de las prácticas informáticas en nuestro país.

En una economía donde la información y el conocimiento se han convertido en una fuente primordial de valor no nos debería sorprender el hecho de que los temas relativos a su distribución apropiación y seguridad ocupen un lugar central en el debate público, la información se ha convertido en un elemento central para la competitividad de las empresas; no obstante la información *per se* carece de valor cuando no es compartida, cuando no es utilizada, distribuida o manipulada.

Lo anterior obliga a las empresas y a las instituciones a integrar bases de datos compartibles, distribuibles y accesibles desde cualquier punto, por lo cual se genera, en principio, la serie de problemas respecto a la seguridad, vulnerabilidad e integridad de dicha información.

En la medida en que el uso de la información se ha convertido en una obsesión, a todas luces justificada por su potencial para fines comerciales o para mejorar la regulación social y política, también se han potenciado los peligros para un ámbito primordial que le da sentido a nuestra convivencia democrática y social, el derecho de los ciudadanos a su privacidad.

Que si bien es cierto en este gran movimiento hacia la digitalización universal, sustentado por los continuos avances de la tecnología, facilita el acceso de los ciudadanos a la información y al conocimiento, haciendo realidad una de las aspiraciones más nobles y democráticas.

El mismo proceso establece una gran zona de conflicto entre las aspiraciones de las empresas y el Estado para el manejo irrestricto de la información y de los derechos de los ciudadanos para hacer valer su privacidad.

De este modo, por ejemplo, el debate sobre la seguridad informática suele plantearse recurrentemente desde la perspectiva de los intereses económicos y crecientemente como un problema de seguridad de los Estados, en la medida en que los intereses de estos actores se hacen valer, a través del lugar privilegiado que ocupan en nuestro orden social.

Las soluciones tanto tecnológicas como jurídicas que responden a estos intereses tienen, en consecuencia, una mayor probabilidad de ser generalizadas y adquirir el estatus de normalidad social, que permite el funcionamiento de un nuevo orden informático digital.

Desafortunadamente no podemos asumir que lo que es bueno para las empresas y para el Estado es, por consecuencia, bueno para los ciudadanos.

En un contexto actual, de gran efervescencia sobre los temas de seguridad y el acceso a la información, los avances en materia de creación de garantías efectivas y procurables para la defensa de los derechos ciudadanos a la privacidad, veracidad y manejo responsable de su información personal, hay un rezago que corre el peligro de que puede convertirse en permanente o normal y, por lo tanto, irremediablemente aceptable.

La capacidad real de los ciudadanos para defender sus derechos no puede ser un asunto menor, en el contexto de la creación de un orden jurídico, alrededor de las prácticas informáticas.

Lo que está en juego es la calidad de nuestra convivencia democrática. Lo que peligra es la vitalidad misma de nuestra libertades y es obligación fundamental que encontremos fórmulas que nos permitan establecer un orden que permita el funcionamiento eficiente de la economía y la regulación social, pero también que garantice a los ciudadanos el respeto a su integridad informática.

Podemos mencionar tres aspectos centrales que deben jugar un papel importante en esta discusión.

El primero tiene que ver con la capacidad de los ciudadanos para hacer valer, de manera efectiva y real su derecho a la privacidad, la integridad, a la veracidad y al manejo responsable de su información personal.

No se trata de un asunto totalmente resuelto por medio de la creación de instancias que regulen el manejo y la transparencia de la información.

La cuestión aquí es garantizar la capacidad de los ciudadanos para gestionar, por sus propios medios, sus derechos. Se trata ciertamente de una capacidad que debe ser establecida jurídicamente, pero también debe de contar con los instrumentos tecnológicos para ser ejercida.

Tomemos como ejemplo el caso de la información financiera y crediticia; mientras que esta información ha estado disponible desde hace décadas y ha generado a su alrededor una impresionante arquitectura tecnológica para su manejo y manipulación por parte de las empresas del sector, los ciudadanos apenas cuentan con medios para garantizar su integridad y existen notables limitaciones para ejercer cabalmente sus derechos, apenas recientemente sancionados en el marco de la regulación del sector financiero.

Creo que una tarea central en este movimiento hacia la seguridad informática, es encontrar los mecanismos para disolver estas inaceptables asimetrías.

Los ciudadanos deben de contar con medios reales y efectivos para hacer valer sus derechos y el Estado es responsable de garantizar que los instrumentos diseñados para tal fin tengan la más amplia disponibilidad posible.

Esto nos lleva a la segunda cuestión central en este tema, que tiene que ver con la consabida brecha digital que existe entre quienes tienen acceso informático y aquéllos que, por su condición económica o social, carecen de dicho privilegio.

Y nuevamente es una situación donde para hace valer un derecho, es en un principio necesario tener acceso al medio que permite ejercerlo, entonces, el problema pasa precisamente por las garantías mismas para acceder al medio, en este caso a la tecnología.

Y el acceso universal al derecho, a la protección de la información personal tiene inevitablemente un carácter tecnológico y de manejo digital, por lo mismo el problema de la brecha digital debe ser una prioridad del Estado para garantizar los derechos ciudadanos, y no sólo por la no menos importante motivación de permitir un acceso democrático a la cultura y al conocimiento.

Por último, uno de los problemas que amerita una reflexión muy cuidadosa corresponde a la necesidad de establecer marcos jurídicos que no sobrerregulen el entorno económico. Si bien es cierto que debemos establecer marcos que le otorguen claridad y transparencia al ejercicio de los derechos ciudadanos, no podemos imponer obligaciones gravosas a las empresas que requieran de bases de datos personales para su funcionamiento sin desquiciar el desarrollo de nuestra apenas emergente economía digital.

No podemos pasar por alto que somos una de las economías en desarrollo que menos gastan en tecnologías de la información y de comunicaciones, y en consecuencia ya somos un país muy poco competitivo en este renglón.

No podemos establecer sin mayor discusión una legislación que dé una entrada que desincentive a los distintos actores económicos que hacen de la información el flujo vital de su actividad, sin hacerle un profundo daño a nuestra capacidad de generar una dinámica de crecimiento y creación de empleos que nos urgen a todos los mexicanos.

Debemos de reconocer los avances que, como país, hemos hecho en esta materia, tanto en los aspectos que regulan a las instancias gubernamentales, como el que regula la operación de la sociedad de la información crediticia.

Una parte importante de la legislación en materia de datos personales está incluida ya en estos ordenamientos, y creo que antes de que legislemos tenemos pendiente un gran debate nacional sobre lo que debe ser el marco adecuado en la materia.

Creo que debe ser un debate que incluya a todos los actores involucrados, sobre todo, los actores económicos que se sienten afectados por las propuestas legislativas sometidas en estas legislaturas.

Es imperioso también enfatizar lo que está en juego para la vida democrática en este proceso de elaboración de marcos jurídicos de las prácticas informáticas.

Debemos, antes que nada, defender los derechos de los ciudadanos para ejercer efectivamente la defensa de su privacidad, la integridad, veracidad y el manejo responsable de su información personal.

Pero, sin embargo, no podemos hacerlo a costa del desarrollo de nuestras incipientes industrias de información. Nuevamente es necesario que encontremos las fórmulas que den origen a un marco regulatorio que sea equilibrado e

inteligente, pero más aún cuando tenemos la oportunidad inmejorable para construir un orden que justifique las aspiraciones más nobles de una modernidad facilitada por el desarrollo tecnológico y el impulso de una economía digital que abra nuevas oportunidades a miles de mexicanos.

Moderador: Alonso Lujambio Irazábal. Comisionado del IFAI.

David Hernández Pérez, es Secretario de la Comisión de Gobernación de la Cámara de Diputados, una Comisión que juega un papel central en el proceso legislativo relacionado con la iniciativa que proviene del Senado.

Ha ocupado diversos cargos dentro del Partido Revolucionario Institucional, entre otros ha sido consejero político estatal en Jalisco, consejero político municipal en Tlaquepaque, Jalisco, Coordinador de Capacitación en la última campaña de gobernador de Michoacán, Coordinador de Apoyos Didácticos de la Escuela Nacional de Cuadros del PRI; ha sido también Coordinador de Capacitación en el Proceso de selección del candidato del PRI a la Presidencia de la República, coordinador de la Federación de Estudiantes de Guadalajara; miembro fundador de la Agrupación Política "licenciado Enrique Díaz de León", de Jalisco; miembro fundador de Vanguardia de Profesionistas Jesús Reyes Heroles; es psicólogo, es experto en neurolingüística; tiene también una trayectoria empresarial, es propietario de la empresa Artes Gráficas.

Ponente: David Hernández.

Decirles que la LIX Legislatura retomó la minuta que en origen presentó el senador García Torres a finales del año pasado, de 2004. Y sí, efectivamente estaba, como se dice ya comúnmente por ahí, en la congeladora, la sacamos a petición de él mismo, él fue el que nos recordó que ahí estaba y nos dimos a la tarea de empezar a trabajarla.

Por parte de la Cámara de Diputados ya hemos realizado dos foros muy provechosos. Nos hemos dado a la tarea de escuchar de una o de otra forma opiniones de los diversos grupos para evitar en lo más lo que se ha venido diciendo, de que por lo regular hacemos las leyes dentro de la Cámara y detrás de los escritorios.

Pero es cierto, en la Cámara de Diputados como en todos lados, hay opiniones diferentes, opiniones encontradas, los hay en la propia casa de cada uno de nosotros.

Cuando nosotros no queremos ir a dormir la señora quiere ya que estemos ahí acostados. Y por cierto que a veces es cuando más gastamos, cuando ya estamos dormidos algunos de los señores.

Decirles que nosotros estamos entre algunos dilemas. Por ejemplo, si el IFAI es realmente sea quien debe de manejar esto que para nosotros es más amplio que lo que viene manejando el IFAI. Es cierto, tiene una gran experiencia; el IFAI ha dado muy buenos resultados, tiene una estructura que se puede utilizar, pero nosotros estamos valorando, si no debiese ser al revés, si no debiese ser que las actividades que está realizando el IFAI en estos momentos debe de ser parte de un Instituto que tendría que realizar actividades mucho más amplias.

Y ya lo decía el senador García Torres, en el sentido de que la diversidad que puede haber en la producción de datos de cada uno en lo educativo, en lo laboral, en lo económico, como funcionarios públicos, en cuestiones médicas y más aún allá, en lo genético, que de una u otra forma ya con el Instituto de Genoma Humano que próximamente podremos tener, no un mapa, sino una resonancia magnética de cada uno de nosotros en donde podamos saber qué tipo de medicamentos nos funcionan, qué tipo de medicamentos pueden ser mejor para nosotros, cuándo vamos a tener qué tipo de enfermedades y una serie de cuestiones que pueden ser útiles para una aseguradora para no darnos alguna prestación o para un patrón para

no contratarnos y una serie de cuestiones que están puestas ahí dentro de la mesa y que tenemos que estar valorando.

Eso es lo que prácticamente el estado en el que estamos ahorita y que también estamos valorando algo que se nos ha venido comentando y que estamos nosotros de acuerdo en que debe ser el propio interesado quien a final de cuentas diga no permito que mis datos circulen de un lado para otro; porque si lo hacemos como está planteado en origen, en donde automáticamente ya nadie puede moverse, pues acabaríamos, de entrada, con muchos empleos de muchas empresas de mercadotecnia.

Sí tenemos que buscar la forma de sí proteger los datos personales, pero también garantizar comercios, garantizar la posibilidad de que también a mí me llegue la información que yo quiero, que yo necesito, que yo puedo permitir en determinado momento y esto tendría que hacerse a partir precisamente de la petición del interesado. Y tenemos que buscar también esa forma.

También tenemos que buscar la forma que si ya hay una serie de datos que nosotros dimos y está en poder de equis banco, por ejemplo, y que con letras muy pequeñas decía que él tiene derecho a otorgarlos y porque ya lo firmamos, entonces ya puede él hacer cualquier uso de esos datos, bueno, tendríamos que poner una limitante en cuanto a eso y tendría que pedir en determinado momento la autorización. Estamos analizando todo eso.

El presupuesto que tendría que destinarse, por ejemplo, si se creara un Instituto.

Claro, que tendría que incrementarse adicional bastante, probablemente, depende de la estructura que se pudiera crear, todo dependería ya del espacio, nosotros estamos preparando ahorita una propuesta de dictamen con varias posiciones en donde tendremos que invitar a una mesa en cortito ya para poder platicar no tan amplia con todo respeto, para poder llegar a algunos acuerdos en donde podamos entonces sí decir qué es conveniente, si de entrada que el IFAI se haga cargo con la estructura que tiene y dentro de un Transitorio que se prepare la creación de un Instituto para que éste absorba todas estas actividades en un futuro e ir avanzando con pasos firmes sin necesidad de crear un monstruo que a final de cuentas no rinda los frutos que esperamos.

Nosotros estamos, como fracción priísta, completamente de acuerdo en sacarla en este período. De hecho platicábamos con nuestro coordinador la semana pasada, con un grupo de empresarios incluso, hemos platicado también con otros compañeros legisladores y están puestos en que la sacaremos en este período, pero tendremos que sacarla con las características que les hemos comentando y ahorita no hemos decidido, vamos a analizar la propuesta, incluso, junto con los compañeros senadores para que no suceda de que nosotros le hacemos las modificaciones y luego se va al Senado y resulta que nos la regresan.

Entonces, ya una vez, la semana próxima que tendremos nosotros nuestra propuesta y que lo platiquemos ya con nuestros compañeros senadores en un trabajo bicameral podamos tomar una determinación, entonces, invitaríamos de nuevo a una mesa para ultimar detalles.

Y ese es el estado que guarda que principalmente era lo que yo quería comentarles en esta importante reunión.

Moderador: Alonso Lujambio Irazábal. Comisionado del IFAI.

José Cipriano Gutiérrez Vázquez, Diputado de la LV Legislatura del Estado de México. Es licenciado en Sociología de la Universidad Autónoma Metropolitana, con un postgrado en finanzas públicas en el Instituto Nacional de Administración Pública.

Es actualmente como diputado Vicecoordinador de Política Económica y Finanzas Públicas, del

Grupo Parlamentario del Partido de la Revolución Democrática.

Ponente: José Cipriano Gutiérrez Vázquez.

Quienes ejercemos hoy función pública que delibera y decide sobre la configuración de leyes, la configuración de marcos normativos, tenemos entorno un tema tan de vanguardia en nuestro país y tan necesario de discusión en términos de lo que la realidad actual obliga a México y evidentemente a los estados.

Yo quisiera dividir mi participación, si ustedes me lo permiten, en dos partes:

Uno. Lo que sería el comentario que se me solicitó sobre la ley propiamente de protección de datos personales y otra que corresponde a un tema de circunstancia Orteguiana, en términos de realidad concreta como diputado del Estado de México, que tiene que ver precisamente con un problema esencial y fundamental de datos personales.

Abordaré el primer tema diciéndoles que cuando se me invitó a comentar, a hacer un comentario y una opinión sobre el estado de la cuestión de la protección de datos en nuestro país, tenía yo varios cuestionamientos: en marcar el problema, revisar lo realizado hasta este momento, en términos de marcos normativos.

Pero es precisamente hoy, con la exposición el senador Antonio García Torres, que se me clarifica mucho más este tema, porque para mí tiene en este momento dos componentes esenciales en el caso mexicano.

Uno que tiene que ver fundamentalmente con el área conceptual, doctrinal y evidentemente legal para transformar el marco normativo y otra que tiene que ver con el aspecto instrumental de quién es, cómo se hace, cuánto se le asigna de presupuesto para tener esta función.

En el caso del marco conceptual y doctrinal, decía yo, me queda muy claro hoy en la exposición que hace el senador, porque aunque con la clarificación que él ha hecho en términos de los modelos americano y europeo, yo no quisiera referirme a eso, sino a dos elementos, dos marcos que nos pueden ayudar.

Evidentemente la necesidad de protección de los datos personales nace con una necesidad económica de contenido económico. Eso es algo que no se cuestiona: La protección de las bases de datos, la transferencia, etc., pues es en términos comerciales, en términos económicos.

De hecho ya aquí se ha mencionado, todo esto de lo que nos dimos cuenta en nuestro país, la venta de los bancos de datos, etc. O sea, tienen un fin económico comercial.

Pero en los últimos tiempos, en los últimos momentos, se ha introducido otra variante, otro elemento, otra vertiente, que son los derechos civiles, los derechos ciudadanos, y esto también corresponde ya, quizá, a la entrada de la cuarta generación de los derechos civiles o ciudadanos.

Más allá de los civiles, de los políticos, de los económicos, hoy tenemos éstos de la protección de la privacidad, del problema de la publicidad de los datos.

Entonces tenemos dos componentes esenciales en esta discusión, tanto conceptual, doctrinal y legal: Una que tiene que ver con todo lo que es la economía, con todo lo que es la necesidad económica, el momento que vivimos de la sociedad informatizada, de la digitación de la persona, etc. Toda esa discusión teórica, política que tiene que aterrizar en un marco normativo.

Y me parece que es importante rescatar y no dejar de enfatizar que en México debemos aprovechar, si bien tenemos un rezago de muchos años, no debemos dejar de aprovechar la oportunidad de introducir, con toda responsabilidad, el marco de los derechos civiles y ciudadanos, de la protección de la persona, de la intimidad, de la honorabilidad de la persona.

Si en las discusiones que se estén llevando a cabo en la Cámara de Diputados Federal este

componente no tiene un peso específico, seguramente vamos a tener muchos problemas posteriores, por elementos que voy a comentar más adelante.

Pero me parece que este elemento es fundamental de enfatizar: Sabemos que hay una necesidad económica de la protección de los datos personales, en términos de lo que hoy es el comercio internacional y las necesidades económicas del siglo XXI.

Pero si no tomamos en consideración los derechos civiles, los derechos ciudadanos, la protección a la intimidad, estaríamos haciendo un marco normativo cojo y un marco normativo anticuado, un marco normativo que se desliga de la realidad que estamos viviendo hoy.

En el caso de la componente instrumental, es cierto, hay un, digamos, el mayor escollo que se está teniendo en términos de avanzar en la legislación, en ya tener el marco normativo es quién va a aplicar esa norma, quién va a aplicar esa regulación. ¿Será algo superior o que contenga la transparencia? ¿O la transparencia debe contener la regulación de esta ley de datos personales?

No es un tema menor tampoco, pero es un tema eminentemente de componente político.

Es un tema de cuál es la institución. Creamos una institución nueva que compagine con el IFAI, creamos una institución o le damos atribuciones al IFAI, para que regule esto a partir de esa ley, o creamos un organismo o una institución que contenga al IFAI dentro de sus funciones, que contenga las funciones también del IFAI y adicionándole las funciones de regulación en términos de la Ley de Protección de Datos Personales.

Es un tema político, y como aquí el diputado a lo mejor ahí lo tendrán que discutir los diputados federales, que son en este momento a quienes les corresponde la discusión, quizá no es un tema fácil de tratar en un encuentro como éste, pero me parece que sí hay que puntualizar que ahí está el problema político, de los juegos de poder y de la creación de instituciones. Y ahí es donde está detenido el problema.

Porque ya el problema presupuestal es menor en términos de la resolución del problema político, de quién será la instancia que regule. Pero eso se tendrá que discutir, se tendrá que resolver. ¡Ojalá! como aquí se ha expresado, en este mismo periodo ordinario de sesiones para que podamos ya, los estados, empezar a trabajar, si es que es una ley federal, en lo que corresponda en el ámbito de cada quien.

Me parece a mí, ahí me atrevo a dar mi opinión, que el IFAI puede ser la institución que tenga bajo su responsabilidad, la aplicación y vigilancia de esta ley, de esta ley federal que pudiera resultar de la discusión política dentro de la Cámara.

Yo sería partidario de que el IFAI fuera la institución que estuviese regulando y vigilando este nuevo ordenamiento. Pero es una opinión particular, que con responsabilidad, con respecto me atrevo a hacer en esta mesa.

Y decía yo esto en cuanto al comentario general, evidentemente la ley, desde mi punto de vista es necesaria por cuestiones económicas, por razones económicas que son evidentes hacia todos, necesitamos, insisto, darle un peso específico al componente de la preservación o la vigilancia de los derechos civiles, los derechos humanos y ciudadanos. Me parece que eso tiene que estar dentro de la discusión.

Y tercero, me parece que el Instituto, el IFAI, debiera ser la instancia que regulara y vigilara este ordenamiento.

Hasta ahí yo dejaría este comentario en términos generales, pues todo lo demás, ya aquí hemos escuchado, están los especialistas, están quienes están discutiendo la ley en concreto.

Nosotros en el Estado de México no tenemos todavía esta discusión. Acabamos de terminar una discusión sobre el área de transparencia,

seguimos discutiendo la Ley de Transparencia, todavía.

No tenemos muchos elementos para abonar en términos muy concretos de lo que está sucediendo en el Estado de México. Pero me atrevo yo a dar esta opinión, dado que se me solicitó en estos términos.

Pero decía que también esta invitación a discutir o a opinar sobre una ley de protección de datos personales se me hace en momento de una circunstancia muy particular que tiene que ver con datos personales, que tiene que ver con la publicidad de ciertos datos sensibles, para utilizar ya la terminología *ad hoc* en que se está utilizando en términos de la discusión de la propia ley de protección de datos personales.

Y yo me preguntaba, decía, cómo es interesante esta invitación a participar, porque tenía yo en mente bajo este problema que todos conocemos, un escándalo político en el Estado de México, cómo hemos venido trabajando con muchos traspiés y con muchas desconfianzas en la conformación de la democracia mexicana, la democracia en México.

Tenemos 10 años en una lucha que va desbrozando el camino de estas desconfianzas, desvelando estos intrincados pasadizos de la conformación de marcos normativos de la democracia, donde la Ley de Protección de Datos Personales es, sin duda alguna, un elemento sustantivo.

No hace mucho, una década, la desconfianza sobre los procesos electorales nos obligó a una discusión profunda, extensa, intensa para conformar instituciones como hoy lo tenemos en el Instituto Federal Electoral. La desconfianza sobre los procesos electorales nos obligó a discutir las reglas para el acceso al poder, la transparencia, la confianza en los procesos electorales.

Todavía hoy tenemos discusiones sobre el propio Instituto, creo que no vamos a dejar de tenerlo, es una institución pública en donde se toman decisiones importantes y como tales siempre son discutibles.

Pero avanzamos hacia finales de la década de los 90 y se nos presenta otro gran problema de la construcción de la democracia en México, que es la transparencia, la duda sobre el ejercicio del poder y del gobierno, sobre el ejercicio de la función pública, qué hacen y como lo hacen quienes son funcionarios y quienes son servidores públicos.

Nos lanzamos a una discusión teórica, conceptual, política sobre la transparencia y logramos establecer una Ley de Transparencia que hoy todavía sigue siendo discutida tanto a nivel federal como a niveles locales. Todavía no terminamos en los estados de la República para que todos tengan una ley correspondiente a la federal en términos de transparencia y acceso a la información.

Y si bien nos explicaba el senador que fue presentada la Ley de Protección de Datos Personales antes que la Ley de Transparencia. Hoy, con las realidades que estamos viviendo, las circunstancias que estamos viviendo nos damos cuenta que hoy, incluso, tenemos un problema de credibilidad en el ejercicio de la función pública a través de la cuestión de los datos personales en términos patrimoniales y de transacciones financieras.

Por eso les decía es azaroso este camino de la confianza que es uno de los elementos fundamentales de la democracia en nuestro país. Pero, bueno, así están las cosas, así lo hemos venido haciendo, la desconfianza de los procesos electorales, la duda sobre el ejercicio del poder y del gobierno, y hoy la circunstancia de la duda y de que se tiene que hacer en términos de los datos personales en términos patrimoniales y transacciones financieras de quienes han ejercido la función pública o la representación popular.

Y por eso decía que es un tema que me hace reflexionar porque nosotros lo tenemos en el Estado de México y, sin duda alguna esto nos

obliga a revisar, no sólo atender la creación de una Ley de Protección de Datos Personales con las connotaciones que ya he mencionado anteriormente, sino nos obliga a revisar los marcos normativos en términos de la Ley de Servidores Públicos, de la obligatoriedad, de la presentación de los datos patrimoniales y hoy de la discusión sobre si también es necesario y posiblemente obligatorio que quienes ejerzan función pública o representación popular tengan que hacer públicas sus transacciones financieras y patrimoniales.

Porque eso me parece que es un reclamo necesario, la realidad está ahí, la duda se siembra en la ciudadanía y tenemos que responder. Y tenemos que responder en base a instituciones y en base a marcos normativos que definitivamente hoy tenemos pero que nos resultan insuficientes.

La Ley de Transparencia del Estado de México nos permite un marco de solicitud de información sobre estados patrimoniales de funcionarios públicos y sin embargo las instituciones no tienen esa agilidad o no tienen esa voluntad política que se debe tener también para cumplir la ley.

Necesitamos revisar esos otros marcos normativos que son complementarios o que son incidentes en la creación de una ley federal o una ley general de protección de datos personales.

¿Hasta dónde los datos personales fundamentalmente patrimoniales y de transacciones financieras de servidores públicos, de representantes populares o ex funcionarios o ex representantes deben ser públicos? Y me parece que esta es una discusión que tendremos que dar en México porque así lo requiere la construcción de nuestra democracia, la consolidación de nuestra democracia.

Hoy ahí está la duda, hoy ahí nos surge la inquietud y tenemos que atenderlo con instituciones y con marcos normativos.

Si no le damos una respuesta correcta por la vía institucional y legal a este tipo de circunstancias no estaremos abonando en mucho en la creación de la confianza en nuestro país, en nuestros gobernantes, en nuestros representantes, no estaremos abonando en la transparencia, no estaremos abonando, sobre todo, en la protección de los datos personales de los ciudadanos en general.

¿Por qué? Porque los ciudadanos en general también tienen patrimonio, tienen transacciones financieras y necesitan la confianza en un país que esté gobernado con transparencia y con confiabilidad.

Ese es un tema que me surge a mí, que me hace reflexionar a partir de la discusión de una Ley de Protección de los Datos Personales en este tema, porque la realidad los rebasa y la realidad mexicana como se ha dicho muchas veces, rebasa las fantasías y rebasa los surrealismos.

Y ahí lo tenemos y tendremos que reflexionar en ello.

Moderador: Alonso Lujambio Irazábal. Comisionado del IFAI.

Álvaro Canales Gil fue Secretario General de la Agencia Española de Protección de Datos y es actualmente Subdirector General de Inspección de la propia Agencia Española.

Ha colaborado en diversas publicaciones sobre el tema, entre ellas *La Agencia Española de Protección de Datos Personales, Estructura y Funciones*, publicada en la obra *La Protección de Datos en Iberoamérica*, publicado en Valencia en el año de 2005. En este año se ha publicado otra obra en Madrid coordinada por él que lleva por título *Código de Protección de Datos*.

Ponente: Álvaro Canales Gil.

Estoy muy orgulloso de estar aquí representando a la Red Iberoamericana y también a la Agencia Española de Protección de Datos.

Y es para mí un tremendo honor que hayan tenido la generosidad de poner a disposición de un miembro de la Red y de un miembro de la Agencia Española de Protección de Datos el dar una opinión y establecer una programación de principios y garantías que se puede deducir o se puede analizar desde el punto de vista de la tramitación parlamentaria de la Ley Federal de Protección de Datos de los Estados Unidos Mexicanos.

Lo primero que quiero decir es que la intervención quiero hacerla meramente descriptiva, lanzando una serie de interrogantes y analizando una serie de deducciones que no vienen del propio texto originario, a mi juicio, de febrero de 2001, como nos ha explicado el senador García Torres, sino que ya surge antes, surge antes del acuerdo de la asociación económica, concertación política y cooperación firmado entre la Comunidad Europea y los Estados Unidos Mexicanos en el año 2000.

Como se ha dicho, en la evolución de la normativa de protección de datos en los Estados Unidos Mexicanos existe desde la presentación del proyecto García Torres hasta nuestro días una serie de regulaciones específicas en materia de protección de datos, hemos oído hablar en estas jornadas de la ley del año 2002, de los servicios de las sociedades de la información crediticia que se aprobó en enero de 2002 y hemos oído hablar mucho y tendido de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, de junio de 2002.

Pero digo que antes de este proceso existe este acuerdo entre la Comunidad Europea y México, y en este acuerdo del año 2000, en su artículo 51, se dice que "las partes convienen en garantizar un grado elevado de protección respecto al tratamiento de los datos de carácter personal y de otra índole, de conformidad con las normas adoptadas por los organismos internacionales competentes en la materia y por la comunidad".

Continua diciendo el artículo 51, en su punto dos, "a tal efecto, las partes tendrán en cuenta las normas contempladas en el anexo".

Acudimos al anexo y allí encontramos que las normas de referencia de las más significativas de entre las cuatro que menciona, están el Convenio 108 del año 1981 del Consejo de Europa y la Directiva 95 46 del Parlamento Europeo y del Consejo del 24 de octubre del año 1995, quienes hayan seguido las sesiones de ayer, lo han citado otros ponentes y ha sido tratado específicamente por el miembro del Consejo que nos acompaña en estas jornadas.

En esos instrumentos lo que todos ellos señalan es una serie de principios y una serie de garantías y de derechos que se reconocen al titular de los datos de carácter personal.

Por citarles el primero de los instrumentos que he mencionado, el Convenio 108, en los principios básicos de protección de datos trata del principio de calidad, trata del principio de seguridad, trata también del principio de información, artículos 5, 7 y 8 del propio Convenio 108.

Y hablando de derechos a los ciudadanos denomina a estos derechos, derecho de conformación, derecho de comunicación y derechos de rectificación y borrado.

Asimismo, la Directiva 95 46, que precisa ya amplia los principios contenidos en el Convenio 108, vuelve a establecer una ampliación y vuelve a pormenorizar y avanzar en el terreno abierto por el Convenio 108.

Por tanto, yo creo que los Estados Unidos Mexicanos al haber firmado ese acuerdo, han apostado por una serie de principios, por una serie de garantías que están recogidos en estos instrumentos.

Y, por tanto, no se trata en este modelo, al cual han prestado su consentimiento de apostar por un modelo europeo o por un modelo norteamericano.

Yo entiendo que se trata de apostar por un modelo mexicano, en el sentido de que lo que compartimos los europeos es un foro común, un factor común de principios y garantías.

Y luego cada Estado, en el momento de transposición de las Directivas, en el momento de reglamentar en el ordenamiento jurídico interno aquella parte del derecho comunitario que nos vincula establece su propia configuración interna.

Por tanto, voy a hacer referencia a estos principios que disciplinan y que además han sido mencionados nuevamente en la Reunión de Montreux de este año, del año 2005, como unos Principios que deben de ser comunes a todo proceso de regulación en materia de protección de datos, en este caso en Montreux referido a la globalización y a la protección de datos de carácter personal.

Se ha dicho que en definitiva la protección de datos de carácter personal tiene un contenido económico y es un contenido económico que yo creo que es innegable. Las empresas necesitan datos de sus clientes, necesitan datos de nuevos clientes, necesitan datos de proveedores, necesitan hacer introspección de nuevos mercados y eso es fundamental para que sigan creciendo y ampliando su balance de resultados, su cuenta de resultados, sus dividendos y su progresía.

Debe de ser respetando y entrando en unas reglas de juego que cada Estado y en este caso los Estados Unidos Mexicanos pienso que lo deberán hacer así, estableciendo un determinado modelo, optando por un sistema de *Opt-in*, en el sentido de que estos principios del Derecho Comunitario y del Convenio 108 del Consejo de Europa, apuestan por el consentimiento del interesado y una serie de excepciones a este principio, que deben de estar establecidas en una norma con rango de ley, porque estamos hablando, lo hemos dicho hasta la saciedad en estas jornadas, de un derecho fundamental a la protección de datos de carácter personal.

Por tanto, con estos principios en el tema de la protección de datos de carácter personal, aquel que trata el dato asume y tiene que demostrar y asumir la carga de la prueba, de que el tratamiento de datos que ha efectuado es conforme a la norma.

Es decir, que tiene el consentimiento del interesado o que hay una habilitación legal que le permite tratar ese dato sin el consentimiento del interesado. Este es un planteamiento muy genérico, pero es un tratamiento en la esencia y en el factor común del modelo que describo.

Me gusta mencionar el siguiente asunto: En algunos Estados el dato sensible es el dato económico. Yo he oído en alguna ocasión que la protección de datos aplicado al sector financiero es absolutamente inviable.

E oído también en relación a este comentario que la protección de datos acabaría con el secreto bancario.

Yo les planteo la siguiente cuestión: Si no existe una normativa horizontal de protección de datos con el modelo y las características que el Estado decida, cualquier persona, cualquier agente que pueda comprar libremente en el mercado cualquier tipo de base de datos puede utilizarlas para cualquier tipo de actividad legal o ilegal, y para esta actividad no necesita saber qué saldo o qué valores tiene un determinado señor, una determinada familia en una cuenta bancaria, simplemente entrecruzando una serie de datos, especialmente relevantes o seleccionados, se puede saber, creo que con bastante precisión si una persona, una familia tiene una determinada posición económica y patrimonial, y por tanto es susceptible de configurar el perfil que la gente que está haciendo ese cruce de datos pretende obtener.

En un entorno de ausencia de regulación si sobre los datos personales existe un innegable valor económico, lógicamente los sectores que trabajan en este ámbito, están absolutamente felices, absolutamente cómodos sin cumplir ningún tipo de obligación, y por tanto muchas

veces intencionadamente se confunde la protección de datos con otra serie de parámetros que el propio sistema de protección de datos admite excepciones al régimen general y horizontal de aplicación a la globalidad del sistema.

En cuanto a la situación en los Estados Unidos Mexicanos tenemos, por un lado, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Es decir, tendríamos una norma con rango de ley que regularía todo el acceso a esta información pública de carácter federal.

Existe también una ley de las sociedades de la información crediticia, entidades crediticias del año 2002, sí tendríamos otra norma con rango de ley que regula este tipo de sociedades de la información. También tendríamos otra serie de sectores excluidos de la propia normativa de protección de datos, como puede ser el régimen electoral, en el cual a pesar de estar excluida la normativa de protección de datos, como creo que su propia norma indica aquellos detentadores, partidos políticos que acceden a esa relación electoral para afrontar unos nuevos comicios tienen que no desviar la finalidad para la cual la obtuvieron, y por tanto el resto que queda de regulación de otros sectores públicos y de los sectores privados, es lo que sería objeto, en principio de esta regulación de la Ley Federal de Protección de Datos de carácter personal en los Estados Unidos Mexicanos.

Yo he descendido un poco al texto de la norma del proyecto, y advierto algunas cuestiones que no me voy a resistir a comentar.

Por un lado, la norma tiene como objeto garantizar los derechos de los ciudadanos mexicanos.

Sin embargo se observa en la norma que no se sabe muy bien cuáles son los contornos concretos, de qué derechos dispone concretamente el ciudadano mexicano, porque se citan en diferentes partes y yo he optado por hacer caso y relatar los derechos que se recogen en el artículo siete, en la fracción cuarta cuando habla de los derechos de acceso, rectificación, actualización, complemento y supresión de datos de carácter personal.

En segundo lugar. En el ámbito objetivo se excluye una serie de sectores, de ámbitos, unos de los cuales son las bases de datos de titularidad pública cuyo objeto por ley, sea almacenar datos para su publicidad con carácter general.

Yo no sé cómo están reguladas, lo confieso, las normas sectoriales que regulan esta materia y si es así que hay una norma habilitante con rango de ley que dice que la información de esos registros públicos es accesible en su integridad por cualquier tercero, no tengo nada que decir.

Lo que sí digo es que nosotros en la aplicación de este apartado tenemos la definición de un concepto, que es el concepto de interés conocido, es decir, la manera en la cual modula aquél que administra los datos, si aquel tercero que le solicita un dato de un titular tiene legitimación y tiene justificación suficiente para pedirle esos datos que le está solicitando a ese registro que tiene naturaleza pública, pero que en modo alguno su norma constitutiva permite un acceso indiscriminado de terceros a esa información.

También les quería comentar algunos aspectos del proyecto que se refieren a datos que aparecen publicados en medios de comunicación oficial. Entiendo que estos datos que se publican en medios de comunicación oficial tendrán la consideración de fuente accesible al público y por tanto de esa naturaleza se derivaría que cualquier tercero puede tratar los datos sin el consentimiento del titular.

Creo que es una cuestión que planteo la incógnita o la pregunta porque no estoy seguro de que esto sea así.

En cuanto al esquema de principios, el principio del consentimiento, en cuanto a la recogida de los datos, es una garantía fundamental, es decir, el consentimiento inequívoco del titular se basa

en que aquél que trata los datos, que recoge los datos, que los almacena, que los recopila, que los recolecta tiene que informarle al titular de los datos de qué datos recaba, con qué finalidad, para qué, si hay sesiones previstas, etcétera.

Y aquí en el proyecto se hace una estructura inversa en el sentido de que no se recoge expresamente esta información en el momento de la recogida de los datos, pero sí se recoge el derecho del ciudadano a solicitar al responsable que le facilite la información sobre los mismos extremos a los que se refiere la directiva 95 46 de la Comunidad Europea.

Por tanto, creo que no sería muy congruente el *pibotar* una información sobre unos requisitos para dilucidar un consentimiento inequívoco que no estuviese previamente habilitado por una cláusula de recogida de datos.

En penúltima cuestión que les quería plantear respecto al modelo y a los principios, insisto, del acuerdo del año 2000 entre la Comunidad Europea y los Estados Unidos Mexicanos, me gustaría hacer referencia a esta cuestión, a la cuestión de los datos sensibles.

Respecto de los datos sensibles dentro de los cuales se recogen los datos de salud, se establece la necesidad de un consentimiento expreso y por escrito y, sin embargo se dice que este consentimiento no es preciso, simplemente cuando se vaya a facilitar al ciudadano una asistencia médica, una prevención o un diagnóstico médico sobre su estado de salud.

Pero no se relaciona esa falta de consentimiento en el momento de tratar los datos sensibles sin el consentimiento del titular, no se relaciona con una situación extraordinaria que se produzca en al salud del propio interesado, cosa que sin embargo sí se dice cuando se habilita la posibilidad de la transmisión de esos datos de salud a un tercero.

Creo que en este apartado, respecto al tema de los principios que relativa en un principio sería oportuno recapacitar.

Por último, les quería plantear una cuestión que sé que puede ser delicada, pero creo que debo mencionar a la hora de analizar el proyecto. Y es la figura de las sociedades de información, porque he dicho que en el año 2002 se aprobó la Ley de Sociedades de la Información Crediticia, es una norma que tiene un ámbito bien concreto como nos lo han explicado en la sesión anterior y sin embargo, aparece esta figura de las sociedades de la información respecto de las cuales el proyecto no identifica con empresas que se dedican al marketing directo ni a la prospección comercial y tampoco se identifican con las sociedades de información crediticia.

Se establece un filtro, una autorización administrativa previa del Gobierno Federal para constituirlas, como una posibilidad de incluso las autoridades fiscales les proporcionen datos y, sin embargo, en algunos casos a estas sociedades de información crediticia que hacen informes o reportes sobre determinados ciudadanos se les permite facilitar, obtener datos de salud en contra de las normas de transmisión de datos que establece el artículo 23 en su fracción II.

Por tanto, quiero hacer mención a este tipo de sociedades, no sé si son sociedades de la información de carácter crediticio llevadas a cabo por entidades comerciales, por empresas, no sé si se refiere a otro tipo de sociedades de información, reconozco mi ignorancia en este asunto, pero les quiero plantear estas cuestiones respecto al estado y situación del crédito.

Como conclusión les quería volver al origen de mi intervención. Creo que por encima no, pero también como un documento complementario a las iniciativas llevadas a cabo tanto en el Senado, como en el Congreso de Diputados, no convendría perder de vista este acuerdo de asociación económica, concertación política y cooperación entre la Comunidad Europea y los Estados Unidos Mexicanos, porque creo que en ese instrumento ratificado por México tenemos una referencia a una serie de principios y de garantías que pueden modular perfectamente el modelo de protección de datos mexicanos y

en definitiva en un futuro llegar a obtener por parte de los Estados Unidos Mexicanos el reconocimiento de un nivel de protección adecuado y equivalente al de la Unión Europea.

Moderador: Alonso Lujambio Irazábal. Comisionado del IFAI.

Antes de pasar a dar respuesta a varias preguntas que ya están aquí entre nosotros, creo importante rescatar una idea central de la exposición última de don Álvaro.

La búsqueda del modelo mexicano. Creo que estamos en una coyuntura histórica en el desarrollo de este derecho en el mundo, en donde se abre un espacio extraordinario a mi juicio para la creatividad; armonizar estos valores que insistentemente hemos estado analizando creo que es el gran reto.

Y a mi juicio si México lograra resolver de algún modo creativamente esta tensión, armonizarla, creo que se pondría a la vanguardia de este debate y creo que de algún modo la iniciativa del senador apunta en ese sentido, quizá, con algunos matices si se quiere o desarrollos más puntuales de algunas normas.

Yo debo decir, por otro lado, respecto de un tema que ha estado aquí en la mesa y lo digo con transparencia, porque esa es una obligación de esta institución, que en el IFAI ciertamente sobra decir esto: no somos grupo de presión, somos autoridad responsable.

Lo que yo les he querido transmitir a nombre de la institución senadores federales es que en el IFAI tendríamos la mejor disposición de asumir esa nueva responsabilidad, una responsabilidad pública que supone la aprobación de una nueva Ley de Protección de Datos Personales.

Hemos analizado la experiencia francesa de dos instituciones que ha generado colisión, hemos visto la experiencia inglesa reciente, la de algunos estado de la federación canadiense, en donde la fusión en una institución de estas dos responsabilidades ha sido exitosa.

En todo caso, quiero expresarles nuestra mejor disposición para compartir los datos que tenemos, esa es nuestra prioridad de contribuir constructivamente a su debate, diputado, senador.

Si les parece bien me gustaría que procediéramos a dar respuesta a las preguntas que ya he distribuido, en el mismo orden en el que ustedes fueron interviniendo a lo largo de esta deliberación.

En consecuencia, le pediría a Francisco Javier Acuña que diera breve respuesta,

Ponente: Francisco Javier Acuña.

Me toca a mí atender el comentario del doctor Julio Téllez Valdés que es investigador de jurídicas de la UNAM y que como él lo dice aquí hago énfasis a los señores legisladores y en este caso, por lo pronto, a los señores diputados les corresponde el turno de dar una respuesta de gran entidad a un tema que tiene que ser atendido porque no puede, eso sí, quedar en el aire, no puede quedar estancada la oportunidad de resolver el asunto en forma adecuada.

Ya lo decíamos, en el Estado democrático siempre se ha resuelto primero el tema de la protección de datos personales e incluso el tema del acceso y la transparencia a la información pública.

En algunos lugares ha sido simultánea la experiencia y ha sido afortunada.

México emprendió una ruta distinta. Este foro demuestra que hay un compromiso creciente por dar a esta cuestión ya una salida, esperamos que decorosa.

Y de esta manera pedimos a los señores legisladores que, en consonancia a su responsabilidad gravísima sobre la cosa pública, incidan favorablemente y tomen de este foro las mejores recetas, para adecuar su creación, la creación legislativa que necesitamos.

Ponente: Antonio García Torres.

Aquí está una pregunta que dice: ¿Considera importante que el futuro Instituto de Protección de Datos Personales sea regulador y también poseedor de los datos personales o usted qué piensa?

Yo le contestaría que de acuerdo con el proyecto y aquí ha habido una confusión en muchas personas interesadas en el tema.

El Instituto, si es que se crea, no tiene como función recabar los bancos de datos que existen en este país que, por otro lado, yo quiero decirle que son miles y miles de bancos de datos.

Cualquier profesionista tiene un banco de datos. Cuando uno va con un doctor le pregunta en dónde vive, su teléfono, dónde lo puedo localizar, sus parientes, a quién le avisamos, y un profesionista va formando un banco de datos.

De acuerdo con el proyecto de esta ley, si ese profesionista esos datos los va usar sólo para el ejercicio de su profesión, no tiene ninguna obligación de registrar ese banco de datos.

Si él va a transmitir los datos personales entonces sí ya tiene la obligación, primero, de registrarlo ante el Instituto y después de pedir la autorización del titular de los datos.

Pero esto es por señalar un ejemplo. Cualquier cadena de tiendas, de restaurantes, de hoteles, todos tienen bancos de datos que hoy en día en México no sabemos ni cuántos son ni para qué los usan ni quién los maneja ni qué destino les dan a los datos de cada quien. Por eso la importancia de tener esta ley.

Entonces, aclarando, no hay la obligación de que el Instituto tenga todos los bancos de datos. El Instituto va ser el órgano regulador para saber cuántos bancos hay, dónde están, quiénes son los responsables de los bancos, quiénes recolectan, para capacitar, para informar, para corregir esos datos, cuando el interesado sienta que lo están afectando con datos falsos o con datos que no están correctos, para ampliarlos, en un momento dado, hasta para solicitar su cancelación.

Entonces, aquí sí que quede muy claro que el Instituto no va ser el dueño de todos los bancos de datos ni va a recolectar los bancos, no; cada quien tiene su banco y lo maneja.

Lo que el Instituto va a manejar es nada más cuál es el banco, en dónde está, quién lo maneja, para qué lo utilizan.

Tengo otra pregunta que dice que si considera usted que para reformar o complementar una Ley de Datos Personales o promover la autorregulación sea necesario legislar en forma clara y específica en materia de daño moral.

Yo creo que sí, yo les diría que tengo por ahí presentada una iniciativa sobre reformas en cuanto al daño moral y que también es algo que estoy impulsando. Definitivamente sí lo creo muy importante y muy necesario.

Hay aquí otra pregunta más, que en lo más central dice que se está trabajando con tres borradores sobre esta Ley de Datos Personales.

Yo aquí quiero decirles, a reserva de que el señor diputado también tome la palabra en este tema, que solamente hay una minuta que fue aprobada por unanimidad en el Senado de la República a la que me referí en mi exposición y que fue turnada a la Cámara de Diputados en el año 2002.

Que después de esa minuta, yo en lo personal he seguido trabajando el tema, he asistido a muchos foros internacionales, he estado en Buenos Aires; he estado en Guatemala también, invitado por el doctor José Luis Piñar. Colaboradores de mi oficina han asistido a otros foros en Cartagena de Indias y en Madrid, porque hemos tenido un gran empeño en que esta iniciativa llegue a feliz término, y que México cuente con esta legislación.

Hay una minuta en Cámara de Diputados y hay un documento de trabajo, que así yo le he denominado, para no llamarle ni siquiera anteproyecto, porque este tema ya está en la Cámara de Diputados y ellos son los que van a dictaminar. Lo que yo he pretendido es que el dictamen que ellos saquen en un momento dado ya vaya con el conocimiento de nosotros lo senadores, para que como él lo dijo, ya no nos lo estemos peloteando; sino que como ellos lo aprueben al regresarlo a Cámara de Senadores, nosotros también lo aprobemos y ya pase a ser ley.

Hay la minuta y un documento de trabajo en el que ha participado mucho el Banco de México, por conducto del Banco de México la Secretaría de Hacienda y últimamente también la Secretaría de Economía. En un afán de lograr la uniformidad de criterios.

Son nada más esos dos documentos, y yo también relaté que el documento de trabajo lo hemos facilitado a los sectores interesados, a las gentes que manejan redes de Internet, de software, de marketing, de todo, para que den su opinión, y para que si esta ley sale finalmente vaya lo más ampliamente conocida, y sobre todo a los sectores a los que va destinado.

Ponente: David Hernández.

A los comentarios que hace el senador. Efectivamente, no tenemos un documento. ¿Qué es lo que hicimos? La minuta que nos envía el Senado con las observaciones que nos envía posteriormente el senador García Torres, con la información que nos han estado haciendo llegar en los foros algunos de los participantes, nosotros estamos elaborando una propuesta.

Y ese será, en determinado momento el documento sobre el que se tendrán que hacer las discusiones. Gracias.

Ponente: María Eloisa Talavera Hernández.

Tengo dos preguntas. Una del señor Héctor Guerrero Huertas, que pregunta si habrá algún trabajo conjunto para impulsar esta iniciativa de datos personales, pero que esté equilibrada antes de dar un dictamen final.

Y hay otra del señor Everardo Maldonado Martínez, que pregunta: Desde el 2001 se presentó la iniciativa, y que cuáles son las causas por las que no se ha aprobado.

Debo de mencionar que en efecto la minuta está en la Comisión de Economía y está turnada también a la Comisión de Gobernación.

Y no es que no haya un consenso al interior únicamente de la Cámara de Diputados entre los grupos parlamentarios.

Yo creo que va más allá por el tema que se plantea y las dos perspectivas que se plantean en la discusión de esta minuta o de esta ley, que tiene que ver con la protección de los datos personales, el garantizarle al ciudadano la seguridad, pero también cómo lo hacemos compatible con toda una actividad comercial que se viene desarrollando en el país, y que como lo mencionaba hace un momento, es incipiente, va naciendo y en principio hemos estado trabajando, preguntando, consultando con usuarios interesados de esta ley también de protección de datos personales, y me refiero pues a las cámaras de la industria electrónica, a las cámaras de mercadotecnia, a las asociaciones bursátiles, entre otras.

Lo que nosotros hemos levantado con ellos también es que se requiere de un análisis mucho más profundo del tema y para poder tener una decisión que sea verdaderamente consensuada.

En ningún momento del proceso de esta ley, por ejemplo, se ha invitado a la industria a participar en la elaboración; yo creo que estos foros son importantes porque se abre el tema de discusión y se recaban las opiniones de todas las partes que se ven afectadas también con la construcción de un instrumento tan importante como es esta ley.

También hay preocupaciones importantes con respecto a la iniciativa. Hay obligaciones, por ejemplo, a quienes se dediquen a vender productos, obtener un consentimiento previo y expreso de los individuos para poderles enviar información o transmitir datos. Y otra serie de cuestiones.

Establece también facultades discrecionales a la autoridad con el fin de definir una tecnología a emplearse en el manejo de archivos. Y tiene varias implicaciones; es decir, para que un individuo pueda tener acceso a información referente a una promoción directa de bienes y servicios, y/o servicios, tendrá que enviar primero su consentimiento a cada empresa; que no es lo que precisamente ocurre en el mundo.

Hay afectaciones que esta iniciativa propicia, por ejemplo que a lo mejor si se plantea así como está, pues sí que haya una inhibición a la economía y que se afecten a empleos que se tienen ahorita y que además son necesarios.

Dentro de las propuestas que nosotros estamos manejando, trabajando en la misma Comisión, y debo de decirlo también, al interior del mismo Grupo Parlamentario es precisamente recoger opiniones de los sectores involucrados y poder llegar a un consenso con esta ley, si haya que modificarla o construir otra.

Creo que nos falta trabajo, pero que es importante abrir una discusión plural y escuchar a todas las partes para poder consensar un instrumento que pueda balancear las dos cosas: la protección o la seguridad que tenga el ciudadano de su información personal, pero también que se llegue a un balance en la parte del desarrollo de la economía. Gracias.

Ponente: José Cipriano Gutiérrez.

A mí se me pregunta sobre si hay deficiencias en la Ley de Transparencia en el Estado de México, no tanto en el marco normativo, yo más bien encuentro algunas deficiencias y resistencias todavía en la operación propia de la ley.

La ley, yo creo que fue una discusión muy amplia, muy intensa, habrá que ver primero la factibilidad de operación de la propia, no diría yo en el marco normativo, creo que es reconocido ampliamente que la Ley de Transparencia del Estado de México es una ley que incorpora las discusiones actuales y trata de ser un instrumento normativo de vanguardia.

Sí hay la posibilidad de que se expida en el Estado de México una Ley de Protección de Datos Personales. Evidentemente que es factible que se dé, obviamente no existe todavía una iniciativa presentada, me imagino y sé que mi amigo y compañero en la Cámara Luis Gustavo Parra pues estará preparando alguna cosa similar, estaremos discutiéndolo y evidentemente atentos a lo que resulte de la discusión en la Cámara de Diputados Federal.

Por otro lado se me pregunta si yo considero oportuno que el Instituto de Transparencia del Estado de México tenga facultades para castigar o sancionar a las personas que violen la Ley de Transparencia.

Insisto, esto sería una discusión posterior a la operación, a la verificación de la operación de la ley. No podemos dar, otorgar nuevas facultades o rediscutir la ley cuando todavía estamos en el plan o en el momento de la implementación de la propia norma, por lo que esto será una discusión posterior.

Yo creo que estamos en vías de conseguir ya el consenso y la voluntad de todos los actores para que la Ley de Transparencia en el Estado de México sea una realidad y, bueno, posteriormente discutir tanto sus deficiencias, como sus reformas.

Ponente: Álvaro Canales Gil.

Bueno, tengo dos preguntas, la primera pregunta es: ¿Cuáles han sido las adecuaciones que han sufrido las leyes españolas de bases de datos y qué razones han influido sobre estas adecuaciones?

La respuesta que yo le daría a don Gerardo Guerrero, es el que hace la pregunta, es la siguiente: En cuanto a leyes españolas de bases de datos no se puede hablar propiamente de esto, lo que habría que hablar sería de leyes españolas que en algún punto concreto y debido a un bien jurídico a proteger o a prevenir o especialmente a hacer un tratamiento de datos en condiciones excepcionales al principio del consentimiento, habilitan a que el responsable de esa base de datos efectúe los tratamientos sin ese consentimiento siempre y cuando el legislador lo quiera hacer.

Por lo demás, desde el año 1999, a partir de enero del año 2000 que entró en vigor la Ley Orgánica de Protección de Datos, es la que disciplina en términos generales y horizontales, todo el funcionamiento del sistema y establece la posibilidad de un acceso, comunicación de datos siempre y cuando estén tasados una serie de motivos que aparecen en la propia ley orgánica, es decir, la norma genérica y horizontal y las normas sectoriales lo que hacen es ir siguiendo el ítem que les he relatado al principio, que es un principio de consentimiento en términos generales con algunas habilitaciones legales que hacen causa o crisis de ese consentimiento, bien porque las refleja expresamente una ley sectorial o bien porque exista un caso de excepción como puede ser la relación de una relación contractual o negocial asumida por el titular de los datos y que hace preciso el tratamiento de datos sin ese consentimiento.

En cuanto a la segunda pregunta dice: Parece que se observan dos vertientes en el Encuentro, por un lado, el problema que origina las instituciones financieras al usar los datos personales de los usuraos y, por otro lado, el surgido con la solicitud de datos personales de servidores públicos para conocer la información que los gobiernos no han dado a conocer de manera oficiosa o que han clasificado. ¿Cómo quitar el aparente antagonismo que interpretan en este sentido?

Yo les puedo decir la experiencia española y es lo siguiente: las instituciones financieras tienen que tener, vuelvo al planteamiento anterior de principios que es el que en definitiva a los estudiosos, a los licenciados en derecho nos hace observar y dar solución a los temas.

Las entidades financieras tienen que tratar los datos siempre que tengan alguna habilitación para ello, es decir, si un cliente tiene un determinado producto financiero y de ese producto financiero que ha contratado no se deriva la emisión por parte del banco en un determinado o nuevo producto, ese tratamiento será un tratamiento sin consentimiento por parte de esa entidad financiera.

Cosa diferente es si la institución financiera, porque no especifica la pregunta a qué se refiere exactamente, puede incorporar los datos de deudores a un buró de crédito.

Cosa que sí permite la Ley Horizontal, la Ley Orgánica de Protección de Datos como una serie de garantías y de prevenciones que el propio caso específico contempla a la hora de volcar datos de deudores y buscar la solvencia patrimonial de futuros clientes que esa entidad decide evaluar para establecer nuevos riesgos a su gestión.

Por otro lado, respecto a la información de los gobiernos, pues aquí volvemos a plantear otra vez el tema de los principios, es decir, si una materia es clasificada, una materia está exenta, no está recogida dentro del derecho de información que tiene el titular de los datos, lógicamente esa habilitación legal permitirá que el órgano federal en este caso o central en el caso autonómico o local en el caso español, imposibilite el acceso a ese tipo de datos.

Piensen ustedes lo verdaderamente esperpéntico que supondría que un terrorista que sabe que existe una base de datos, lógicamente de ficheros terroristas ejerciera un derecho de información a obtener los datos que la policía o las fuerzas de seguridad del Estado tienen de él.

Y piensen también el esperpento que supondría su aplicáramos el modelo general y yo he relatado antes si a un terrorista, o un narcotraficante, a un grupo de delincuencia organizada cada vez que hubiera que introducir un dato en un fichero de esa naturaleza hubiera que informarle: consiente usted que... pues, lógicamente caeríamos en un tema absolutamente ridículo.

Por eso digo que el modelo permite compartiendo principios adaptar esos principios que son la base fundamental de la estructura jurídica a la problemática concreta que exista en un determinado país, como he relatado anteriormente.

Presentación del Libro: Privacidad y Derechos Humanos 2005

Presentador: Vamos a continuar con la presentación del libro que se refiere a la protección de datos de carácter personal en Iberoamérica, le doy la palabra al doctor José Luis Piñar Mañas.

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

En lo que a mí me atañe y como Presidente de la Red Iberoamericana de Protección de Datos, es un enorme honor y una gran satisfacción poder presentar hoy ante todos ustedes y en el marco del VI Encuentro Iberoamericano de Protección de Datos una publicación que es fruto del trabajo de la Red Iberoamericana de Protección de Datos.

La Red Iberoamericana de Protección de Datos surge en el año 2003, en la ciudad de La Antigua, en Guatemala. Allá se celebra un Encuentro de Protección de Datos Personales los días 2 a 6 de junio de 2003. Encuentro del que surge una declaración, la llamada *Declaración de La Antigua*, que consta de nueve puntos, uno de los cuales, el punto número siete es precisamente el de la creación de la Red Iberoamericana de Protección de Datos.

Y en ese punto, en el punto número siete, entre los compromisos que asume, los cometidos que asume la red, se encuentra el de promover la edición y publicación de documentos de trabajo y de las obras que permitan difundir y dar a conocer los resultados obtenidos en el desarrollo de las actividades de la Red Iberoamericana de Protección de Datos.

De la letra de la declaración pasamos a la acción y esa acción se ha concretado en la obra que hoy tenemos el gusto de presentar ante todos ustedes.

Se trata, en efecto del libro *Protección de Datos de Carácter personal en Iberoamérica*, que ha sido editado por la propia Red Iberoamericana de Protección de Datos, junto con la Agencia Española de Protección de Datos y una de las más prestigiosas editoriales jurídicas de España, la editorial Tirant lo blanch.

Este libro, del que tienen ustedes aquí algunos ejemplares, recoge los trabajos del encuentro al que antes me refería, el Encuentro celebrado en La Antigua, Guatemala, en junio del 2003.

Es una obra que pretende hacer ver que la red no sólo se manifiesta a través de declaraciones, a través de trabajos de enorme importancia, a través de la vía de fomentar, dar a conocer el derecho fundamental a la protección de datos personales, sino también a través de obras concretas, que

permitan a todos aquellos que quieren acercarse al derecho fundamental, a la protección de datos, tener un instrumento de información que les permita conocer la situación que en la materia se da en diversos países.

Este libro consta de dos partes bien diferenciadas. La primera está dedicada a lo que hemos denominado estudios generales; la segunda, la que se dedica a estudios nacionales.

Dentro de los estudios generales hay diversos trabajos que se refieren a cuestiones de carácter general, que tienen que ver con el derecho fundamental a la protección de datos.

Y en este sentido se abre con un trabajo de quien les habla, sobre el derecho fundamental a la protección de datos; a continuación un estudio sobre la evolución histórica y el marco normativo internacional del derecho fundamental a la protección de datos.

A continuación un trabajo de don Fernando Argüello, quien ha intervenido en este Encuentro, sobre protección de datos personales, *La Directiva Comunitaria, su influencia y repercusiones en Latinoamérica*.

Seguido de un estudio del doctor Juan Antonio Travieso, que también ayer tuvo ocasión de dirigirse a todos ustedes, sobre la protección de los datos personales en América Latina: *Unidos o Desprotegidos hacia una Red Iberoamericana de Datos Personales*.

A continuación un trabajo de don Jesús Rubí Navarrete, también ayer tuvo ocasión de intervenir en este Encuentro sobre *Tratamiento de datos personales en la prestación de servicios de telecomunicaciones*.

Otro más de don Emilio Aced, sobre transferencias internacionales de datos, y dos más en particular sobre cuestiones de carácter general, por más vinculadas al área iberoamericana y América Latina.

Por un lado un *Estudio sobre la conferencia iberoamericana, su sistema de cooperación y la protección de datos personales* y otro sobre *MERCOSUR y la protección de datos*.

Esta primera parte, por tanto, configura lo que sería los contenidos generales de la protección de datos personales.

La segunda parte se refiere, o se dedica a estudios nacionales, estudios de Colombia, a cargo del doctor Nelson Remolina; de la República de Costa Rica, a cargo del doctor Alfredo Chirino, también ha intervenido en este Encuentro y del doctor Mario Carbajal, que también nos acompaña, así como de don José Francisco Bart.

Estudios también de España, a cargo de Mar Martínez y de don Álvaro Canales.

También dos estudios de la situación en protección de datos en México, uno de ellos precisamente sobre el proyecto de Ley Federal de Protección de Datos Personales, redactado por el senador Antonio García Torres, quien es un miembro muy activo de la Red Iberoamericana de Protección de Datos, y otro sobre la legislación sobre protección de datos personales en México, redactado por don Eduardo Guerrero Gutiérrez.

Hay también un estudio sobre Paraguay, que se encargó de elaborar la Superintendencia de Bancos de Paraguay. Otro sobre Perú, elaborado por la doctora Lilián Oliver, y dos más sobre Uruguay, uno de ellos elaborado, redactado por el entonces senador, doctor Alberto Brause, y otro por la doctora Ana Brian, que también interviene en este Encuentro Iberoamericano de Protección de Datos.

Creemos que es una primera muestra de lo que quiere ser la Red Iberoamericana de Protección de Datos, un foro de encuentro, de intercambio de experiencias, de intercambio de información, que pretende facilitar la información a todos cuantos se mueven en el sector de la protección de datos, ya hemos dicho innumerables veces durante este Encuentro de un derecho

fundamental de todos y cada uno de los ciudadanos.

Junto a este libro querría también hacer una brevísima referencia a otra mucho más modesta, pero no por ella menos importante publicación de la red, que es la que contiene las declaraciones hasta ahora aprobadas en el marco de la Red Iberoamericana de Protección de Datos, y que se les han entregado a ustedes como parte de la documentación de este Encuentro.

La primera de ellas, de enorme importancia es la que tuvo lugar con ocasión de la Declaración de Santa Cruz de la Sierra, en la Decimotercera Cumbre Iberoamericana de Jefes de Estado y de Gobierno de noviembre de 2003, en la que se hace una referencia expresa en el punto 45 a la protección de datos personales y a la Red.

Permítanme muy brevemente leer este punto 45, que considero de enorme importancia:

Dicen unánimemente todos los jefes de estado y de gobierno de los 21 países iberoamericanos reunidos en Santa Cruz de la Sierra en Bolivia.

Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos, contenidas en la declaración de la Antigua por la que se crea la Red Iberoamericana de Protección de Datos abierta a todos los países de nuestra comunidad.

Por tanto reconocimiento expreso de que la protección de datos es un derecho fundamental. Reconocimiento expreso también de la importancia de la Red Iberoamericana de Protección de Datos.
Además, se recoge la declaración de la Antigua a la que antes me refería y también la declaración de Cartagena de Indias con motivo del encuentro celebrado en mayo de 2004, que recoge las conclusiones que entonces se alcanzaron en la Red referidas a temas de enorme importancia en nuestra opinión.

La primera de ellas sobre *La protección de datos y la perspectiva del sector financiero*.

La segunda. *La lucha contra el Spam*.

La tercera. *Las transferencias internacionales de datos, perspectivas Europea e Iberoamericana*.

La cuarta. *El sector de las telecomunicaciones e Internet ante los ataques de la privacidad*.

La quinta. *El sector comercial y el uso de la información con fines de marketing*.

La sexta. *Consideraciones en torno al desarrollo de la Red Iberoamericana de Protección de Datos*.

Es intención de la Red el acometer de inmediato la publicación, no sólo de estas declaraciones, sino también de la que surja de este encuentro, del Encuentro México 2005, al objeto de completar de este modo una publicación de mayor alcance incorporando todos los documentos que hasta ahora se han producido en el ámbito de la Red, no sólo en texto español, sino también traducidos al inglés para dar una mayor difusión a todo lo que en materia de protección de datos se está haciendo en el ámbito de la comunidad iberoamericana.

Tan sólo me resta agradecer muy de veras a todos cuantos han participado en la redacción de este libro y de estos documentos, por su tesón, por su infatigable labor, por su impulso y por su ánimo, desde que en junio del 2003 en una reunión que debo decir entonces era sumamente sencilla, me atrevería a decir, una reunión de no muchas personas que creíamos que había que dar una expresión de apoyo a todo cuanto se está haciendo mucho y bien en materia de de protección de datos en Iberoamérica, de una expresión del grupo que entonces surgió a lo que es este IV Encuentro Iberoamericano de Protección de Datos.

Agradecimiento a los que han colaborado en la Red, los que están colaborando en la Red. Agradecimiento a todos los que han participado

como autores del libro que ahora tengo el honor de presentar.

Y por último, y por supuesto agradecimiento a quienes han organizado, al IFAI sobre todo por habernos permitido presentar este libro en este Encuentro.

Y agradecimiento una vez más a todos ustedes. Tan solo decirles que disponemos de algunos ejemplares, pocos, pero quien tenga interés en esta obra, puede ponerse en contacto o bien con el IFAI o bien con la Agencia Española de Protección de Datos Personales.

Cédric Laurant: Consejero de Política, Director, Proyecto de Privacidad Internacional, Electronic Privacy Information Center-EPIC.

Les presentaré el libro y voy a hablar sobre los desarrollos globales que se llevaron a cabo en el período en que este libro se hizo desde junio del 2004 hasta julio del 2005.

Este libro proporciona una visión general del los temas más importantes de privacidad, desde la supervisión de satélites, del comercio, etc., y también revisa el estado de privacidad en más de 70 países en todo el mundo.

En la primera parte que se llama *Visión Global* que nos habla sobre lo básico de lo que es la privacidad, de lo que quiere decir privacidad e instituciones de protección, de cómo definir la privacidad, cuáles son los modelos de protección de privacidad.

Existen secciones que nos hablan sobre la vigilancia, la vigilancia de la comunicación, el consenso, la privacidad, la privacidad de los viajes, etc.

Y también hay una tercera parte sobre los informes de los 73 países que hemos analizado este año y en estos informes nosotros hemos tratado de dar una presentación, una introducción sobre el marco constitucional que se refiere a la privacidad a la protección de los datos y de la privacidad de las leyes criminalísticas y las de procesamiento criminal y también en los países donde dichas autoridades existen.

Y también incluimos algunos países como Nueva Zelanda que han ratificado en la Comisión Internacional los derechos de privacidad.

En este año también tuvimos una organización que incluida puntos muy breves sobre los desarrollos más importantes en esos países, las gráficas que incluyen las leyes de protección de privacidad en cada uno de los países, un glosario de recursos de privacidad internacional, que se pueden encontrar en diversos países, si ustedes quieren investigar más y cuáles son las informaciones que ya existen, las informaciones que hay en el libro. Y también tenemos una versión en CD.

Para la elaboración de este libro nosotros trabajamos con más de 200 expertos, desde profesores, académicos y autoridades de protección de datos, funcionarios del gobierno, activistas de derechos humanos, activistas diversos y personal diverso.

También les voy a hablar sobre lo que yo creo es lo más importante o el desarrollo más importante que se llevó a cabo en los últimos 12 meses.

Esta investigación más bien se enfoca en la supervisión del gobierno y en las acciones gubernamentales, en la privacidad de cómo responder ante la amenaza del terrorismo.

Primero vamos a hablar de uno de los desarrollos más importantes que son las medidas que el gobierno tomó y realizó para responder frente a terrorismo y también de otras medidas gubernamentales de bases de datos de información de salud y de uno de los desarrollos más importantes en los últimos 12 meses en el campo de supervisión de privacidad y de identificación y tecnología de frecuencias de radio.

También hay un cuarto punto al respecto, y quisiera hablar de las leyes de protección de datos en diversos países, de las tendencias de privacidad y sobre los retos más importantes de la privacidad futura.

Lo que hemos encontrado en EPIC, al trabajar en este estudio es que no ha habido muchos cambios en los últimos tres o cuatro años, en especial desde septiembre del 2001 con los ataques terroristas en los Estados Unidos, en Madrid, en Indonesia, en Londres, y también en la forma en que el gobierno ha tratado de responder a la amenaza del terrorismo y también a la forma en que han tratado o han implementado dichas leyes.

Primero parecía que las leyes que se habían puesto en vigor tenían el propósito legítimo y más adelante lo que sucedió fue que una vez que este marco legal ya estaba en vigor, había dado toda la disposición de nuevos poderes a las autoridades de aplicación de la ley y estas leyes se extendieron o estos poderes que se les dieron a las autoridades, de aplicación de la ley, se les dieron de una manera para luchar contra el terrorismo y en contra de otras amenazas, no solamente del terrorismo, sino de otros actos criminales.

Lo que descubrimos en los últimos tres o cuatro años, fue que los países han añadido mucho más de agencias gubernamentales y departamentos gubernamentales, que tienen que ver específicamente con las tareas de luchar contra el terrorismo y de recopilar datos, de coordinar y de compartir información.

Y también hay una retención de los datos, en especial en Europa, pero también en algunos países africanos y latinoamericanos, al igual que la tendencia para centralizar los datos.

Esa no es diapositiva correcta, sino la 1.2, es la siguiente.

Otra tendencia que encontramos es que los gobiernos están dispuestos, con tal de proteger las fronteras, con tal de proteger los medios de transportes, a identificar a las personas en las fronteras.

Primero empezó en las fronteras y después con las revisiones domésticas. Entonces, en principio los países presentaron la idea de supervisar a los pasajeros, de sacarles un perfil y uno de los sistemas más notorios es el sistema estadounidense de seguridad del transporte o sistema de computadora que es como pasar por la pantalla a los pasajeros y EPIC y otros grupos en los Estados Unidos empezaron denunciarlo.

Sin embargo, fue reemplazado adecuadamente por otro sistema y fue una situación que otros países siguieron: Canadá, Australia, la Unión Europea y también algunos países asiáticos.

Lo que yo creo que son los principales asuntos de protección de datos en el caso de este nuevo poder de prescribir un perfil, dado que estas autoridades de aplicación de la ley es el hecho de que más específicamente en el caso de los Estados Unidos, violó las leyes de protección de los datos europeos.

Y, otro caso, que sucedió es que el Gobierno americano protegía sus fronteras y trataba de obtener información a partir de compañías privadas de los Estados Unidos sobre los ciudadanos que vivían, en por lo menos 10 países de Latinoamérica, la información había sido conseguida de una manera ilegal.

Y lo que ocurrió es que la autoridad en los Estados Unidos tomó información de esta compañía privada, compañía local en Brasil, Colombia y México, con tal de ver si había un enfrentamiento entre lo que los inmigrantes habían dicho a estas autoridades fronterizas y lo que los Estados Unidos tenían en sus archivos.

Otra tendencia preocupante es el hecho de que los datos una vez obtenidos por las autoridades de aplicación de la ley y algunas veces la violación de estos datos de protección nacional no está segura de no ser transferida hacia otra

autoridad de aplicación de la ley, que no estaba de acuerdo con esta ley de protección de datos en vigor.

Una situación muy notoria fue la que se llevó a cabo en los Estados Unidos, se llamaba "las visitas de los Estados Unidos", que obligan a todas las personas que entren a los Estados Unidos a dar sus huellas digitales y tomarle una fotografía para poder formar un sistema indicando la identidad de la persona que entra al país.

Específicamente este año nosotros vemos que la mayoría de los países que hemos analizado han salido con ideas o han tenido ideas para cartas inteligentes o tarjetas inteligentes con un número único de identificación, como licencia de manejo, una especie de CURP, huellas digitales, piel, etcétera.

Los principales problemas relacionados con esta presentación de tarjetas inteligentes es que la mayoría de los países que los presentaron no tienen una forma de protección. Eso significa que ellos dan más poderes a las autoridades de aplicación de la ley, sin darles la situación adecuada a otras agencias gubernamentales o grupos de protección al consumidor que tienen la situaron de poder ver si estos poderes que les otorgan los utilizan de una manera adecuada.

Otras medidas gubernamentales que vemos específicamente es la presentación de esta información en la base de datos.

Ya había esta información, pero vemos que cada vez más gobiernos utilizan esta base de datos para poder combatir el terrorismo, y en los países que no tienen esa protección de datos se hace para estos problemas, porque ayuda a que la información médica sea muy sensible a los datos personales, y confía o depende únicamente del gobierno para tratar con esta información, sin abusar de ella y sin diseminarla.

Los poderes adecuados que generalmente no se pueden llevar a cabo, en la mayoría de los países y en especial en los Estados Unidos, lo vimos en muchos casos en donde la información está recolectada por compañías privadas.

Ahora, esto está sin que haya salvaguardas establecidas para poder supervisar las prácticas gubernamentales.

En el campo de lo que es la supervisión del sector privado, una de las tendencias más importantes es el uso de lo que se llama RFID (Identificación de Radio Frecuencia). Esta tecnología realmente no es nueva y se comenzó a utilizar hace como 15 ó 20 años e incluso más en los años 60, pero ahora por el precio tan disminuido de la tecnología y el tamaño tan disminuido de los detectores, hemos visto muchas más aplicaciones que han surgido en lo que es la industria de la defensa.

Se están utilizando detectores de radiofrecuencia para monitorear a los empleados en los lugares de trabajo, para monitorear a los niños en las escuelas, para monitorear a la gente en los hoteles y muchas de estas aplicaciones tienen un rango de precios. Por ejemplo, cuando se tuvo un sistema en Malasia, es una tarjeta inteligente con identificación de radio frecuencia, ésta tenía mucha información sobre la persona y se encontraba en una tarjeta; la de la licencia de manejo, los registros médicos, mucha información.

Lo que está sucediendo más bien, la información de la tarjeta se está centralizando y era muy interesante para *hackers* y gente que roba la identidad.

Quisiera decir que la tecnología de RFID vemos muchas cosas nuevas, lo que son lineamientos, leyes, reglamentos que están trabajando en este campo.

Y también en otros países en donde hay cada vez más industrias, compañías y gobiernos. Esto es un campo en que hay una vigilancia muy intensiva en lo que es la tecnología de identificación de radio frecuencia en la

información financiera y de transacciones, entre asociados, un producto por ejemplo que se compra en la tienda para ver la ubicación.

Lo que quiero decir aquí es que esto se podría utilizar posteriormente para otros propósitos que no están en el sistema de formación de perfiles, y lo que termina sucediendo es que la tecnología comienza con una meta legítima y termina siendo para prevenir cualquier tipo de crimen en un aeropuerto, por ejemplo en Estados Unidos.

Otra tendencia de privacidad es que las autoridades de aplicación de la ley están interesadas en recolectar toda la información que puedan y delegan esta recolección o esta tarea de procesamiento de información a las empresas privadas.

Hay casos muy famosos de los que quiero hablar que son, por ejemplo, una compañía estadounidense llamad Check Point que ayudó a los estadounidenses a obtener información que no podía obtener legalmente, obteniendo esta información de ciudadanos latinoamericanos y mandándola al gobierno. De esta manera se evitaba la aplicación de una ley en Estados Unidos que evitaba que el gobierno obtuviera estos datos.

También encontramos y es difícil llegar a esta conclusión, que la seguridad nacional normalmente se ha detenido por los derechos humanos y los derechos a la privacidad, también la conveniencia.

Un ejemplo, el Departamento de Estado de la Unión Americana, junto con el Ministerio de Relaciones Exteriores de México empezaron a utilizar la identificación de radiofrecuencia en los pasaportes, y aquí la razón principal para hacerlo era la propuesta inicial del Departamento de Estado que fue en diciembre de 2004 y enero de 2005, era poder acelerar el paso de la gente por las líneas fronterizas, aquí se puede ver el valor o la conveniencia que era mucho más importante que el derecho a la privacidad.

Por estas razones creo que los retos siguientes que veremos en la privacidad van a ser pensar cómo los gobiernos y la sociedad civil pudieran establecer unas salvaguardas y supervisiones seguras sobre el uso que está haciendo el gobierno de los nuevos poderes que está obteniendo.

Podemos pensar en las nuevas formas de obtener esta nueva protección con las leyes, esto es potencialmente tecnología muy intrusiva, por ejemplo, sale muy barato como un implante que una empresa pensó en utilizar, y esto indicaría en ponerlo en una persona en el antebrazo, cuando esta persona quedara inconsciente esto llamaría a los paramédicos y a los doctores y esto llevaría información médica del paciente en caso de que él no tuviera un estado adecuado para dar información.

Y en este caso específico, parte de la Unión Europea y algunos lineamientos en países asiáticos no tienen ningún marco de privacidad en vigor, por ejemplo, en Estados Unidos no hay ningún marco de privacidad que aborde estas amenazas de manera específica.

Otro reto de la privacidad sería ver qué es lo que sucede cuando la información que se recolectó de manera legítima y legal en un país tiene que transportarse a otro país, eso crea asuntos de las normas globales de privacidad o flujos transfronterizos de información y este es un gran debate ahora en Latinoamérica, esto se enfrenta con dos modelos básicos: Los modelos en la Unión Europea y el marco del área Asia Pacífico, en la parte cooperativa de Asia Pacífico.

Quisiera evitar los datos, vieran estos importes en las páginas Web en las siguientes semanas o en ésta, está disponible en inglés y a mediados de diciembre en español.

Pedro Mendizábal: Ciudadanía y Derechos en la sociedad de la información, CPSR-Perú.

Para CPSR-Perú es muy grato compartir la presentación en este foro de lo que será la primera edición en castellano del libro

Privacidad y Derechos Humanos, versión correspondiente al año 2005.

CPSR-Perú es un centro de investigación en políticas públicas y tecnologías de la información y comunicaciones, fundado en Lima en octubre de 2002, su misión consiste en promover el uso y desarrollo socialmente responsable de las tecnologías de la información; influenciar en las decisiones vinculadas con las mismas y fomentar el desarrollo de las sociedades de información que concilie la tecnología con el ser humano que la usa.

El campo de acción de CPSR-Perú se sitúa en aquel punto en que convergen tecnologías de la información, derecho y sociedad.

En tal sentido, tiene varias áreas de trabajo entre las que destacan las relativas a derecho de autor en el entorno digital, sociedad de la información, privacidad y protección de datos personales, seguridad de informática, de la información y comunicaciones, entre otras, todas ellas abordadas desde un enfoque interdisciplinario que involucra lo técnico, jurídico, económico, político, social, cultural y ético.

Desde el 28 de septiembre de 2005 CPSR-Perú ha sido incorporado a la Red Iberoamericana de Protección de Datos, como miembro asociado.

La intimidad personal, definida desde la óptica del sujeto que goza y ejerce su derecho, representa el ámbito de libertad del individuo, el momento y lugar en que, como decía Rousseau, lo íntimo de identifica con lo universal.

Ello le permite a la persona reencontrarse consigo misma, recargar energías para retornar con brío a las actividades sociales, en especial trabajo. Es, asimismo, el espacio de sosiego en que toma decisiones que afectarán su futuro y que tendrán, en la sumatoria de millones de intimidades y autonomías, consecuencias de amplios alcances.

La intimidad, pensada desde el individuo hacia el mundo exterior, entendida como espacio de libertad, en el que el sujeto decide en qué medida expone o no su vida privada, disminuye apreciaciones negativas del derecho a la intimidad que lo vinculan, en ocasiones, con el secretismo o individualismo.

Concebido desde esta perspectiva, el derecho a la intimidad se revela no como el derecho del solitario o del ermitaño, sino como el ejercicio de la mínima y necesaria libertad y autonomía que el derecho moderno debe garantizar a la persona humana, para que a partir de su personalidad en acción edifique o público y social.

Por ende, estamos ante un derecho fundamental base de la ciudadanía y dinámicamente relacionado con aquella noción clásica, según la cual el ser humano es ser humano en sociedad.

Lo planteado justifica el esfuerzo por averiguar en 73 países, convocando la participación de más de 200 expertos y colaboradores, durante casi un año de labores, cuál es el estado de la privacidad en el planeta.

La edición en castellano contendrá la parte general del PHR 2005, los reportes individuales de 14 países de América Latina, los capítulos referentes a aquellas legislaciones más influyentes en nuestro medio, como son España, Portugal, Italia, Francia, Alemania y la Unión Europea.

Por relevancia y contraste se ha decidido incluir los reportes de los Estados Unidos, Gran Bretaña y Canadá.

Ahora bien, hemos comenzado refiriéndonos a la intimidad personal y familiar. ¿Cómo se explica, entonces, que el libro que ahora presentamos posea contenidos que exceden largamente el derecho a la intimidad?

Por ejemplo, temas referidos a identidad personal, votación electrónica, privacidad respeto de los datos de viaje, nanotecnología, acceso a la información pública, entre otros.

Interpretado en términos de la tradición jurídica romano germánica, el concepto del *right of privacy* y del *common law*, comprende al menos el derecho a la intimidad personal y familiar propiamente dicho, el secreto de las comunicaciones y la confidencialidad de los documentos privados; la privacidad genética, la privacidad física frente a procedimientos tales como la biometría, el auscultamiento de cavidades corporales, la inviolabilidad del domicilio, la privacidad en los lugares de trabajo e incluso en espacios públicos, así como todo aquello que de una u otra manera proteja la dignidad humana.

El *right of privacy* estadounidense corresponde más a la concepción alemana del derecho general de la personalidad.

El derecho general de la personalidad, entendido como derecho matriz que comprende una amplia gama de derechos innatos, vitalicios, personalísimos, extrapatrimoniales, relativamente indisponibles, nominados o innominados, contenidos o no en el derecho positivo, responde al espíritu garantista de protección de la persona como un todo. Hecha esta breve introducción pasemos a revisar someramente algunos de los resultados fruto de la investigación realizada en latinoamericana.

En la República Argentina, debido a la presión pública por un creciente número de secuestros, se promulgó en mayo de 2004 una ley sobre los servicios de comunicaciones móviles, que eliminó el anonimato en la compra de celulares. La ley obliga a los que venden teléfonos móviles a recolectar la identidad de sus clientes, incluso de aquellos que tienen la modalidad de servicio con tarjeta prepago.

En enero de 2004 el Congreso aprobó la controvertida ley 25873, la misma que modificó la Ley Nacional de Telecomunicaciones de 2003, estableciendo la obligación de las empresas de telecomunicaciones de colaborar con las investigaciones de la justicia, y en concreto, con los pedidos de informes, así como con la obligación de retener ciertos datos de tráfico (telefónicos, por Internet y por cualquier otro medio como la telefonía IP) por el lapso de 10 años.

El reglamento de esta ley generó gran discusión pública. La cámara que agrupa las empresas de telecomunicaciones interpuso una acción de amparo en contra de la aplicación del decreto reglamentario, basándose en los costos que acarreaba el cumplimiento de la medida. Debido a la presión mediática el Presidente Kirchner suspendió el decreto que él mismo había expedido.

En Bolivia se agregó en el año 2004 la acción de Hábeas data al texto constitucional, la misma que se puede seguir mediante un proceso sumarísimo.

En Brasil se han presentado al Congreso varios proyectos de ley. Algunos de ellos obligarían a los proveedores de servicios de Internet y proveedores de alojamiento Web a mantener información personal identificable, tal como el nombre, número de documento de identidad, dirección y teléfono de los clientes, por un plazo de dos a cinco años, así como datos de tráfico de las conexiones individuales a la Internet, incluyendo los números IP de los emisores y receptores de las comunicaciones, cuando se conectan y desconectan a la Internet la cantidad de data enviada y recibida, por un lapso de seis meses a cinco años.

La intercepción ilegal de comunicaciones por parte de investigadores privados, así como la grabación de conversaciones privadas son fenómenos comunes en Brasil. También en 2004, como respuesta a escándalos que involucraban a funcionarios del gobierno federal, el Ministerio de Justicia manifestó su intención de presentar un proyecto de ley destinado a prohibir la intercepción y el uso de la información así recogida, con penas de cárcel para los periodistas que usen cualquier información obtenida a través de dichos medios.

Como reacción a las políticas antiterroristas de los Estados Unidos, que crearon un sistema de

registro de visitantes extranjeros, que comprende el fotografiado y la toma de huellas automatizadas; una corte brasileña resolvió, en reciprocidad, que los ciudadanos estadounidenses también tendrían que seguir similar procedimiento antes de permitírseles el ingreso a Brasil. No obstante la orden de la Corte fue luego revocada, un mecanismo similar fue establecido a través de un decreto del gobierno federal. Hacia finales de 2004, los gobiernos de Estados Unidos y Brasil acordaron mecanismos de cooperación recíprocos sobre la materia.

Respecto del creciente número de cámaras de video vigilancia en lugares públicos y privados, la ciudad de Sao Paulo promulgó una ordenanza municipal que ordena la instalación de signos distintivos, informando de la existencia de tales cámaras, tanto en lugares públicos como privadas. Las imágenes grabadas serán confidenciales, y el incumplimiento de las normas de protección de datos dará lugar a responsabilidad por parte de los infractores.

En Chile se aprobó una Ley de Protección al Consumidor que contiene disposiciones contra el Spam, establece un sistema opt-out y prescribe que todo correo electrónico comercial debe indicar el nombre del remitente, una descripción precisa de lo que ofrece y una dirección válida a la cual el consumidor pueda enviar un mensaje destinado a evitar cualquier futuro E-Mail.

En Colombia existen tres proyectos de *Hábeas data* en discusión, uno de los más controvertidos es el proyecto de ley estatutaria 071 de 2005, presentado por el Ministerio de Hacienda y algunos congresistas. Según el profesor Remolina dicho proyecto deteriora el alcance del derecho fundamental a la protección de los datos personales de los colombianos, fortalece a las empresas que negocian con dicha información y expone a Colombia a que sea catalogada internacionalmente como un país que no garantiza un nivel adecuado de protección a la información personal.

En Costa Rica hay tres proyectos de ley en discusión que regularían el procesamiento automatizado de información personal. La Corte Suprema ha reconocido el derecho a acceder a la información pública a pesar de no estar regulado.

En Ecuador se adoptó una Ley de Transparencia y Acceso a la Información Pública en mayo de 2004 que otorga a los ciudadanos el derecho a solicitar y obtener información sobre actos, contratos y proyectos firmados y financiados con recursos públicos. También en Ecuador se promulgó la Ley de los Burós de Información Crediticia que tiene como objeto regular la constitución, organización, funcionamiento y extinción de las centrales de riesgo. Según la norma legal, la información que obtengan y conserven tendrá por exclusiva finalidad el ser destinada a la prestación del servicio de referencias crediticias y deberá ser mantenida en el país. La información histórica de personas naturales y jurídicas no podrá exceder de seis años; por tanto, a los burós de información crediticia les está prohibido recabar y proporcionar informar posterior a ese límite.

En el Parlamento guatemalteco se presentó en febrero de 2005 un proyecto de ley de acceso a la información pública, clasificación y desclasificación de información en poder del Estado.

En México existen tres iniciativas legislativas referentes a protección de datos personales pendientes de aprobación. La ley mexicana de acceso a la información pública establece como uno de sus propósitos la protección de los datos personales contenidos en ficheros de entidades públicas; creó el Instituto Federal de Acceso a la Información Pública, uno de cuyos fines es la protección de tal información a través de la capacitación a los servidores públicos, la elaboración de estudios y procedimientos.

En el Perú se publicó en la página Web del Ministerio de Justicia, hacia agosto de 2004, un proyecto de ley de protección de datos

personales, que en líneas generales, sigue lo establecido en la normativa europea sobre la materia. Cabe destacar la promulgación en mayo de 2004 de la ley 28/2/37 Código Procesal Constitucional, que regula de manera integral los procesos constitucionales de *Hábeas corpus*, amparo, *Hábeas data*, cumplimiento, acción popular e inconstitucionalidad, sobre todo, porque se trató de una iniciativa privada impulsada de manera espontánea por un grupo de renombrados abogados peruanos que formularon un anteproyecto que con escasas modificaciones fue aprobado por el Congreso de la República.

En abril de 2005 se promulgó la ley que regula el uso del correo electrónico comercial no solicitado (Spam), la norma que se prevé que tendrá escaso efecto práctico establece que todo correo electrónico comercial, promocional o publicitario no solicitado, que se origine en el Perú, deberá contener características específicas de información, tales como la palabra *publicidad* en el asunto del mensaje, el nombre de la persona natural o jurídica que lo envía y una dirección de correo electrónica válida y activa que pueda ser utilizada para la exclusión voluntaria. La ley también dispone una compensación económica para las víctimas del Spam, obliga a los proveedores de servicios de Internet a contar con sistemas de filtro e inusitadamente los responsabiliza (siendo ellos también los afectados) por el Spam que reciban sus clientes.

En Venezuela se aprobó la Ley de Responsabilidad Social de la Radio y Televisión (RESORTE), denominada por la oposición la *ley mordaza*. En general esta ley establece franjas protegidas y programación de contenidos socialmente responsable. También regula la publicidad y prevé múltiples penas en caso de incumplimiento. Más allá de la justificación oficial de la norma como protectora de la población preventiva de la exposición de los niños y adolescentes a la información "inapropiada", la Sociedad Interamericana de Prensa y Reporteros sin Fronteras, han expresado su preocupación por la censura previa y restricciones a la información que la ley RESORTE establece.

En agosto de 2004 y en los meses siguientes la lista de quienes firmaron las planillas solicitando la revocatoria del mandato del presidente Chávez fue hecha pública en la Internet por el parlamentario Luis Tascón exponiéndolos a represalias de parte de seguidores del gobierno.

A manera de reflexión final y mirando el bosque, no sólo aquel grupo de árboles que conforman la jungla jurídica, en la sociedad de la información no son suficientes las normas legales, por más protectoras que ellas sean de los derechos de la persona humana, ni las autoridades de protección de datos, por más dignas e idóneas que sean del cargo que ocupan.

Es sencillo imaginar mil formas de transgredir las normas de protección de datos personales y lo que es peor, es igualmente fácil llevarlas a la práctica de manera impune.

Por lo tanto, si la *etérea composición* es insuficiente, si los procesos administrativos o jurisdiccionales son de probanza imposible, de desenlace incierto o resultado ilusorio, qué nos queda a los ciudadanos conscientes de la importancia de cautelar nuestra data. Pues debemos optar por la prevención y la defensa propia, prevención para no entregar data inconscientemente y sin razón suficiente y defensa propia mediante el uso de herramientas informáticas de auto-tutela o auto-composición que protegen nuestra privacidad y data personal.

Nos referimos, por ejemplo, al uso del correo electrónico seguro, herramientas de navegación anónimas en la Internet, el cifrado de las comunicaciones telefónicas y de los servicios de mensajería instantánea, así como bases de datos y discos duros encriptados.

Pensamos que es relevante que la Red Iberoamericana de Protección de Datos, debata

la posibilidad de ampliar la efectividad de su labor mediante el fomento del uso de este tipo de herramientas informáticas.

Es imperativo trabajar en educación para tener una ciudadanía concienciada y vigilante que premie a aquellos que cumplen con los principios de protección de datos de carácter personal y castigue a los que incumplen dichas normas.

Finalmente, lo más importante, educar en una ética que considere siempre al ser humano como un fin y nunca como un medio.

Agradecemos la cordial invitación del IFAI a la Red Iberoamericana de Protección de Datos y al Instituto de Transparencia y Acceso a la Información Pública del Estado de México por habernos permitido dirigirnos a ustedes.

Medidas de seguridad: Los datos especialmente protegidos

Mesa 7:

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

Los temas que serán abordados corresponden a las medidas de seguridad de los datos especialmente protegidos, a la protección de datos personales en los estados de la República Mexicana y a la presentación de los trabajos de la Red Iberoamericana de Protección de Datos Personales.

Presídium: María Marván Laborde, Comisionada Presidenta del Instituto Federal de Acceso a la Información Pública; Ricardo Sodi Cuellar, Director de la Facultad de Derecho de la Universidad Anáhuac; Luis Alberto Domínguez González, Consejero del Instituto de Transparencia y Acceso a la Información Pública del Estado de México; José Luis Piñar Mañas, Presidente de la Red Iberoamericana de Protección de Datos Personales; Rolando Barrera Zapata, Consejero Presidente del Instituto de Transparencia y Acceso a la Información Pública del Estado de México.

Ricardo Sodi Cuellar.

Es para la Facultad de Derecho de la Universidad Anáhuac, un verdadero privilegio ser sede alterna de este Encuentro Iberoamericano de Protección de Datos Personales, ya que ha sido preocupación de nuestra institución académica, crear espacios de reflexión y análisis de temas tan señalados y de tanta vanguardia, como lo es la protección de datos personales, el derecho a la información, el derecho a informar.

La Universidad Anáhuac y su Facultad de Derecho han establecido varias líneas en este sentido. En primer lugar dentro del programa curricular de nuestra Facultad de Derecho contamos con la materia de Derecho Informático, una novedad que nos pone a la vanguardia académica en este campo de derecho.

Asimismo, en nuestro Instituto de Investigaciones Jurídicas se ha creado una línea de investigación en torno al derecho informático, a la protección de datos personales y la regulación jurídica. De hecho hemos participado con universidades europeas y norteamericanas en el tema relacionado con la protección de datos personales, concretamente el doctor Emilio, de la Universidad Complutense de Madrid, el doctor José Antonio Núñez Ochoa, Director de nuestro Instituto de

Investigaciones Jurídicas han realizado y realizan varias investigaciones en torno a la protección de datos.

Por ello, la Universidad Anáhuac se congratula de tenerlos el día de hoy en sus instalaciones y la Facultad de Derecho considera esto como un día de gran trascendencia para su historia académica, toda vez que crear esos espacios de reflexión en torno a la protección de datos personales, en torno al derecho informático, al acceso a la información es una prioridad de nuestra formación académica.

Les agradezco mucho su presencia, sean ustedes muy cordialmente bienvenidos a la Facultad de Derecho de la Universidad Anáhuac. Espero que disfruten los trabajos de este Encuentro y que sean muy exitosos.

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

Como ha sido ya la mecánica de este evento, vamos a proceder a una Conferencia Magistral a cargo del doctor José Roldán y, posteriormente tendrán su intervención cada uno de los participantes de este panel, que en este momento solamente enumero, María José Blanco Antón, la doctora Marván Laborde, Abraham Sotelo Nava, Enrique Domville y Cédric Laurant.

Iniciamos entonces con esta conferencia magistral del doctor José Roldán de quien brevemente diré algo de su extenso currículum, es un académico reconocido, es licenciado en Derecho por la Universidad Autónoma de Puebla, maestro en Derecho Económico por la Universidad Autónoma Metropolitana, Unidad Xochimilco y, doctor en Derecho por la Universidad Nacional Autónoma de México; ha escrito diversos libros en materia administrativa y sobre otros temas que han sido de su interés y, actualmente es profesor de tiempo completo del Departamento de Derecho del ITAM, titular de la materia de Derecho Administrativo y se desempeñó además como director de la licenciatura en Derecho.

Conferencia Magistral: José Roldán Xopa

Agradezco su gentileza en haberme invitado a ésta que pretenciosamente se llama conferencia magistral; sin embargo, creo que es un buen momento para pensar y procuraré que podamos hacer un ejerció colectivo de pensamiento, tomando en cuenta el estado del arte de la cuestión en nuestro país.

Para nosotros, incluyéndome, resulta novedoso el que comencemos a hablar de un nuevo tema que anteriormente nos parecía hasta cierto punto lejano, pero que con la presentación que diversas iniciativas legislativas en el Congreso sobre la materia nos obliga a pensar mucho más detenidamente y por supuesto en la medida en que vamos entrando al problema vamos, por una parte, en un proceso de conocimiento, pero por otra parte también nos van suscitando diversas pregunta.

Primer punto de entrada, nos importa cada vez que regulamos algo nuevo que la regulación sea efectiva, esto es, que efectivamente, que realmente en la sociedad se provoquen las consecuencias que tiene la intención.

Puede haber muy buenas intenciones, pero si están mal instrumentadas entonces seguramente el resultado va a hacer ineficaz, no se va a lograr lo que se busca.

¿Cuáles serían las condiciones para llegar a tal objetivo? Yo creo que en primer término que la materia se encuentre bien definida. Esto es que se encuentre debidamente precisado qué es lo que se quiere, cuál es el bien que se está tutelando, y por otra parte, además, de la buena definición de la materia, que tengamos una buena organización institucional que instrumente el derecho, que proteja el derecho, que procure el cumplimiento de obligaciones, y por tanto también que tenga un buen sistema de cumplimiento de forzamiento de las conductas debidas.

El siguiente punto es: ¿Entonces de qué estamos hablando cuando oímos el término de datos especialmente protegidos o datos sensibles?

Procuraré hacerlo de una manera muy simple, si en términos generales el término que nos convoca a este seminario es el de la protección de los datos personales, cuando se habla de datos sensibles o datos especialmente protegidos.

Existe una previsión de qué es lo que se considera como datos sensibles. Y lo que dice el proyecto del artículo 19 para que todos podamos compartir esta información, dice: *Ningún titular estará obligado a proporcionar datos sensibles que le conciernen*; y posteriormente dice, *los datos sensibles únicamente podrán ser objeto de tratamiento cuando se cuente con la autorización vigente y por escrito del titular otorgada mediante su firma autógrafa, salvo lo dispuesto en equis artículo.*

Lo que nos está diciendo este artículo es que hay un conjunto de informaciones que está sujeto a una regulación especial.

¿A qué se refiere esto de los datos sensibles? En la Ley, en el Capítulo de Definiciones nos remite a datos tales como la salud, la raza, las preferencias sexuales que, por lo que ustedes pueden ver, presenta una calificación respecto de la valoración o de la posición social del individuo en una sociedad que pudiera dado el contexto de presentar alguna circunstancia particular.

¿Por qué pudiera ser sensible el dato?

La sola expresión de que se hable, por ejemplo, o que se refiera a preferencias sexuales o bien a la salud o a la raza, implica que tal información tiene determinada valoración en una sociedad.

Por tanto, el primer punto, creo, es que el dato sensible depende del contexto en el cual viva el individuo y, por tanto, los datos podrían ser relevantes y ameriten una determinada protección.

En este caso la protección se refiere a un elemento importante que es: No se puede dar a conocer ningún dato que pueda comprenderse dentro de esto, si no es con la autorización de la persona, de su titular, de a quién se refieren los datos.

Lo que podemos ver es una especie de soberanía del titular respecto de la información que le concierne, dependiendo del contexto en el cual se vaya desarrollando.

El primer problema es: ¿Cuáles son estos datos sensibles, cómo se determinan?

Hay un primer problema en la ley. La ley es enunciativa, dice: *Raza, preferencias sexuales, salud, otros y aquéllos que por disposiciones generales determine el órgano encargado de la regulación.*

Por tanto, aquí nos da una puerta, una abertura para que no sea un *númerus clausus*, sino que a través de una decisión administrativa de un órgano regulador se pueda extender el tipo de datos que pudieran ser protegibles. Esto nos plantea una serie de problemas.

Aquí viene entonces la cuestión de la técnica alrededor de la cual se va precisando qué es el dato sensible. Hay una definición legal y, por tanto, después habría una definición administrativa, lo cual crea una serie de problemas normativos.

Voy a entrar a alguna de estas definiciones.

La protección, en buena medida, está encomendada a un órgano regulador. La iniciativa es, hasta cierto punto, ambigua; a veces plantea que puede ser el IFAI o bien algún órgano regulador especializado en esto.

El problema de diseño institucional creo que tiene que entender dos cuestiones: Primero, que los sujetos regulados, si es que tomamos el modelo IFAI, no serían ya la clientela habitual del IFAI, que son entidades públicas, sino que

también serían entidades privadas, lo cual amplía no solamente la clientela, sino que además complica la ordenación, porque en la medida en que hay una relación o bien al interior de la administración o al interior de la organización estatal y al ampliarlo a los particulares, entonces, esto significa que hay una relación externa y, por tanto, la regulación jurídica también es diversa.

Porque las regulaciones jurídicas funcionan de manera distinta cuando el sujeto obligado es un sujeto público, porque hay un relación institucional especial, que no es una relación institucional en donde el sujeto obligado goce de derechos, pero en cambio sí lo es cuando el sujeto obligado, el sujeto regulado es un particular y, por tanto, su posición como gobernado, como administrado, activa una regulación especial y, por tanto, también los medios de defensa y las formas de actuación son distintas.

No operaría de la misma manera una norma general del IFAI que regule esta materia, frente a sujetos públicos que frente a sujetos privados. La exigencia frente a sujetos privados es mayor.

Por ejemplo, podría haber una oposición en el sentido de que la regulación de cuál puede ser el dato protegible debe ser hecho en ley y no por acción administrativa, lo cual evidentemente no podía ser oponible en el caso de instituciones públicas, porque la relación jurídica distinta. Y, por tanto, hay una diversidad de instrumentos y éstos operan de distinta manera si es frente a un particular o frente a una institución pública.

Allí hay que tener mucho cuidado en lo que podría expresarse como una simetría regulatoria.

El siguiente punto es la simetría regulatoria también puede estar complicada debido al tipo de derecho que se cree con la información.

Si un particular argumenta que respecto de la información tiene un derecho patrimonial, entonces el argumento de que se requiere una ley para que pueda consignarse qué dato es el protegible adquiere mucho mayor fuerza. Estoy simplemente señalando problemas.

La siguiente cuestión es el tratamiento, le hace la revelación de la información del dato sensible, está, como ustedes pueden ver establecido como una regla general, solamente con la autorización de su titular puede ser dado a conocer. Este es el principio, que me parece un buen principio, pero sin embargo, tenemos que pensar y preguntarnos respecto de si esto es absoluto.

El propio proyecto establece ya un indicio o un inicio de que esto puede ser relativo en el caso de revelación de datos médicos, esto es, si se requiere para una cuestión de salubridad general o bien de tratamiento específico en la persona puede accederse a esta información.

El ejemplo que me parece muy revelador es el siguiente: Supongamos que una persona llega a un hospital, a urgencias, está inconsciente y, por tanto, no está en condiciones de revelar la información necesaria para el médico, pero el médico requiere llevar a cabo una transfusión sanguínea; entonces, el conocimiento del dato, por ejemplo, de la religión puede ser relevante para el tratamiento, si un Testigo de Jehová, bueno, el médico tiene que enfrentarse al dilema de si opera con una transfusión sanguínea o bien busca otro tratamiento médico alternativo para poder salvar esta objeción, derivada de la religión.

Entonces, suena justificable que haya ahí una salvedad a la necesidad de una autorización previa.

Pero la ley dice que se requiere la firma autógrafa, lo cual plantea un problema de manejo de administración del tratamiento de los datos, a diferencia de lo que pasa con la consignación del tipo de datos que pueden ser regulados en una disposición administrativa, me parecer por ejemplo más razonable que los instrumentos, incluyendo los tecnológicos para poder salvar la autorización con métodos

alternativos a la firma autógrafa podrían ser más propios de una regulación por vía administrativa, tomando en cuenta los avances de la tecnología. Sin embargo, esta es una cuestión que tendría que darse en la discusión.

La pregunta y aquí confieso hasta cierto punto mi limitación de información, solamente en este caso se justificaría una salvedad al monopolio de la autorización autógrafa o pueden existir otras buenas razones para establecer, por ejemplo, que mediante autorización judicial o de alguna otra autoridad diversa a la judicial pueda tratarse, relevarse una información relativa a datos sensibles.

Yo me planteo, por ejemplo, el problema de la raza. En México a partir de la reforma al artículo 2 Constitucional, se establece la raza como un elemento importante para la determinación de determinadas situaciones jurídicas, la incorporación del derecho indígena, el reconocimiento de los pueblos indígenas implica que la raza es relevante para determinadas situaciones, ligadas a obligaciones, a derechos, a preferencias.

La definición de quién es un indígena es por sí misma muy problemática y además es costosa, puede ser algo así como la prueba del diablo. En México con los índices de mestizaje indígena es una cuestión problemática y cara y que en ocasiones no puede ser costeable cuando se va desahogando un procedimiento.

Entonces, ahí puede ser relevante la posibilidad de acceder a una información que puede estar en algún banco de datos público o privado que pueda resolver el problema.

El dato de ser indígena o de ser de otra raza no necesariamente importa o puede no ser viable a través de la autorización de su titular, es más, su titular puede oponerse a que se conozca esa información, pero esa información puede ser relevante para la determinación de una situación jurídica, por ejemplo, para el establecimiento de un agravante cuando se comete un delito.

Si esta información para no acudir a un peritaje médico que puede ser sumamente caro de DNA, por razón de economía de información puede solicitarse a través de algún medio a pesar o en contra de la no autorización del titular.

Nos van surgiendo una serie de problemas que creo que es importante que los vayamos pensando.

Y finalmente es: ¿Qué mecanismos son los que el proyecto de ley prevé para poder tener un adecuado cumplimiento de este tipo de cuestiones?

Partamos de lo siguiente, en la medida en que hay un ordenamiento que regula los datos personales, se lleva a cabo una operación en la cual se excluye del mero manejo de los particulares, y considerando que puede ser una situación de interés público, por tanto, se activa la posibilidad de intervención de órganos administrativos.

Y, además, que la infracción a los deberes tiene como consecuencia la imposición de multas o de sanciones públicas. Esto es, hay una exclusión del menor manejo de relaciones contractuales o defensa o extracontractuales de particulares.

Estamos frente a una cuestión de orden público, en donde la sola infracción, por sí misma, amerita una sanción. Pero la infracción a los deberes de cuidado de los datos personales también puede ocasionar daños particulares.

La pregunta aquí sería: ¿Cuál es la mejor forma o las formas de garantizar un adecuado cumplimiento de deberes?

La ley establece dos tipos de sanciones. Primero, una multa que evidentemente no va a beneficiar al particular. Ni un peso de la multa puede llegar a su bolsillo, pero por otra parte la posibilidad de indemnización si es que hay daño.

Me parecen buenas, me parecen razonables, en principio, estos dos instrumentos. Sin embargo, yo creo que puede quedarse corto. La revelación

de un dato sensible puede ocasionar daños, y por tanto genera la acción de daños y perjuicios. Pero no necesariamente puede generar daños. La revelación de un dato personal puede, inclusive, originar un beneficio a la persona, a su titular, puede darse ese caso. Pero no obstante se violó el deber de cuidado.

Si es así, y si no hay daño, ¿habría alguna acción que tiene el titular, aunque haya sido beneficiado o no haya sido dañado para exigir o pedir una indemnización por el incumplimiento del deber de cuidado de quien tenía ese dato privilegiado o no? Yo sería partidario de que podría intentarse una vía, porque de todas maneras hay una afectación a su decisión de que ese dato no se dé a conocer, independientemente si le origina daño o no.

El siguiente punto, y con eso concluyo, es cómo está diseñada la sanción administrativa. De acuerdo con el proyecto hay una sanción de 5 mil a 10 mil salarios mínimos. La única consideración que hago es que esto nos plantea siempre decisiones de costo-beneficio. Esto es cuánto va del dato personal, el dato sensible.

¿El dato sensible puede valer más de 10 mil salarios mínimos? Yo creo que sí, podría darse el caso de que valiera más. Si vale más entonces la sanción está mal diseñada, ¿por qué? Porque no es un adecuado instrumento para poder inhibir o para poder sancionar una práctica de este tipo.

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

Voy a darle la palabra a María José Blanco Antón, quien es licenciada en Ciencias Matemáticas por la Universidad Autónoma de Madrid, pertenece al Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado.

Se ha desempeñado en diferentes puestos en la Agencia Española de Protección de Datos, ocupando actualmente el de Subdirectora General del Registro General de Protección de Datos.

Ponente: María José Blanco Antón.

La seguridad de los datos y las categorías de datos especialmente protegidos, constituyen dos principios básicos de la regulación de la protección de datos personales, y en los tratamientos de estos tipos de datos la normativa exige una serie de garantías y obligaciones adicionales, a las que con carácter general establece en cualquier tratamiento de datos personales.

El tratamiento de datos especialmente protegidos es uno de los aspectos que plantea mayor complejidad en el análisis general de la regulación de la protección de datos, y esto se debe al hecho de que son tratamientos que conllevan recogidas conservación y uso de datos sensibles, esencialmente relacionados con la esfera más íntima de las personas.

La Directiva Europea de Protección de Datos define las categorías especiales de datos, incluyendo en éstas a aquellos datos personales que pueden revelar el origen racial o étnico de las personas, relativos a las opiniones políticas o con visiones religiosas y filosóficas, la pertenencia a los sindicatos, aquellos datos relativos a la salud o a la vida sexual de las personas y, por último, los relativos a las infracciones o condenas penales o administrativas.

En el tratamiento de estas categorías de datos pueden producirse conflictos entre la intimidad de las personas y, por ejemplo, su esencial derecho a la vida y a la salud, que exige la adaptación, por los ordenamientos jurídicos, de un conjunto de medidas específicas, que garantizando la protección al derecho a la intimidad, a la protección de datos, no dificulte o entorpezca la asistencia sanitaria o médica necesaria, para garantizar los derechos que antes comentaba, a la salud o a la vida de las personas.

La Directiva, cuando establece estas categorías especiales de datos, directamente dice que se prohibirá el tratamiento de estos datos, si bien

planten una serie de excepciones y situaciones, que deja pendiente de que cada Estado en su legislación nacional regule de una forma o de otra, siempre dentro del marco que define la Directiva.

En el ordenamiento jurídico español, la legislación española regula los datos especialmente protegidos en el artículo Siete de la Ley Orgánica de Protección de Datos de la Ley Orgánica de Protección de Datos de Carácter Personal, dentro del Título Segundo dedicado a los Principios de la Protección de Datos. Y define tres categorías de datos sensibles. En primer lugar, los relativos a la ideología, a filiación sindical, religión y creencias, para los que exige que únicamente pueda ser recogidos y tratados si existe el consentimiento expreso y por escrito de la persona, del titular de los datos.

Previamente la Constitución Española, en el artículo 16 fracción segunda recoge que *nadie puede ser obligado a declarar sobre su ideología, religión o creencias*.

La segunda categoría de datos especialmente protegidos que establece la LOPD son los relativos al origen racial, la salud y la vida sexual.

Para esta categoría de datos la legislación española exige el consentimiento expreso de los interesados o bien que exista una ley que por razones de interés general haga preciso el tratamiento de estos datos.

Para estas dos categorías de datos la LOPD realiza algunas precisiones, reconociendo la posibilidad de tratar estos tipos de datos en determinados supuestos, condicionados a ciertas finalidades y a las personas que realizan estos tratamientos de datos.

En cuanto a las finalidades, las finalidades que establece la ley son aquellas relacionadas con la prestación de la asistencia sanitaria o de un tratamiento médico o la gestión de servicios sanitarios o siempre que sea necesario para la prevención o diagnóstico médico.

En cuanto a las personas para las que la ley establece un tratamiento especial, son aquellas, los profesionales sanitarios que se encuentran sujetos al secreto profesional y otras personas que podrían estar sujetas a una obligación de secreto equivalente.

Para estos tipos de datos, además, establece una precisión; el artículo 7 de la LOPD estableciendo que quedan prohibidos los ficheros creados únicamente con esa finalidad exclusiva de almacenar datos que revelen este tipo de información.

Por último, la Ley de Protección de Datos española recoge una tercera tipología de datos especialmente protegidos, que son los relativos a las infracciones penales o administrativas, para los que únicamente las administraciones públicas, competencia en la materia, estarían habilitadas para realizar estos tratamientos de datos.

Por otra parte, como decía a principio, la seguridad de los datos constituye otro principio básico de protección de datos que está también recogido en la directiva y puesto en el ordenamiento español, en la legislación española en el mismo Título Segundo al que hacía antes referencia, dedicado a los principios básicos de protección de datos.

Este principio establece que el responsable de un fichero o el encargado de un tratamiento de datos especialmente protegidos, con algunas precisiones que haré luego más adelante, de cualquier tratamiento de datos, debe adoptar medidas técnicas y organizativas que garanticen la confidencialidad, la integridad y la disponibilidad de la información.

La aplicación de este principio y el nivel de exigencias para evitar la alteración, la pérdida, el tratamiento o el acceso no autorizado, van a ser más amplios en cuanto a la naturaleza de los datos que se tratan sean más sensibles.

Y cuando hablo de datos sensibles, me estoy refiriendo a las categorías de datos especialmente protegidos que he estado citando. Este principio en la regulación española está desarrollado en el Reglamento de medidas de seguridad que aplicando lo que acabo de decir asigna al tratamiento de datos especialmente protegidos, el nivel más alto de exigencias en cuanto a su cumplimiento.

A partir de este momento voy a centrar la presentación en los datos de salud. Para lo que se debería limitar el concepto de datos de salud y cómo se regula.

Es necesario, lo decía yo al principio, evitar conflictos entre el derecho a la privacidad y el derecho a la vida y a la salud y hay que adoptar medidas que garanticen la recogida, la conservación, la confidencialidad, la integridad, la disponibilidad de esta información al resultar esenciales para la preservación de la vida y la integridad física de las personas.

Por ello se hace necesario articular mecanismos que, garantizando la protección del derecho a la privacidad no dificulte o entorpezca la labor médica, la labor sanitaria, la labor investigadora sin el consiguiente perjuicio del interesado.

La importancia de los derechos de las personas, pacientes, como eje básico de las relaciones sanitarias, se han puesto de manifiesto en el interés que han demostrado un gran número de organización internacionales con competencia en la materia como Naciones Unidas, la UNESCO, la Organización Mundial de la Salud, la Unión Europea, el Consejo de Europa que han impulsado declaraciones o han promulgado normas jurídicas sobre la materia.

El Consejo de Europa en particular ha estudiado las cuestiones relacionadas con la problemática del tratamiento de datos en el ámbito de la salud, desarrollando una serie de recomendaciones sobre bancos de datos médicos, sobre el tratamiento de datos utilizados con fines de seguridad social, datos epidemiológicos, datos relacionados con la salud mental. En particular la Recomendación 5/97 sobre protección de datos médicos. La última recomendación que ha estado relacionada con esta materia sobre protección de datos recogidos para fines relacionados con el sector asegurador.

Todos estos son recomendables si se quiere hacer un estudio o realizar una aproximación de los distintos principios de protección de datos y su aplicación en el ámbito del tratamiento de datos sanitarios o en el tratamiento de datos relacionados con la salud de las personas.

Siendo los más importantes, el Apartado 45 de la Memoria Explicativa del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, que viene a ser la primera definición de lo que se considera datos relativos a la salud, incluyendo las informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo, comprendiendo igualmente a las informaciones relativas al abuso del alcohol o al consumo de drogas, pudiendo tratarse de una persona de buena salud, enferma o fallecida.

La Memoria Explicativa del Convenio 108, la Recomendación del año 97 sobre protección de datos médicos también hacen alusión definiendo datos médicos como todos aquellos datos de carácter personal relativos a la salud de una persona, afectando igualmente a los datos manifiesta y estrechamente relacionados con la salud, incluyendo las informaciones genéticas.

Por último, en cuanto a referencias al reconocimiento que precisa la aplicación del concepto de datos de salud, traía una referencia a una sentencia del Tribunal de Justicia de las Comunidades Europeas, que ya ha sido citado en el Encuentro, la conocida como sentencia “linquis”, en la que el Tribunal viene a aclarar qué es lo que se entiende por datos de salud y simplemente hubo una información que publicaba la señora “linquis” en su página Web sobre la lesión en un pie de un compañero de catequesis, el Tribunal deja claro que se trata de un dato de salud.

Volviendo al principio, en el tratamiento de datos especialmente protegidos relativos a la salud, es necesario encontrar ese equilibrio de la aplicación del derecho fundamental a la protección de datos y la prestación de la asistencia médica o sanitaria.

La Ley Orgánica de Protección de Datos en el caso español, la LOPD, establece con carácter horizontal los principios, obligaciones y garantías de protección de datos, incluyendo ya una serie de limitaciones en cuanto al tratamiento de los datos especialmente protegidos; la normativa de protección de datos se completa con la Legislación Sectorial y la armonización de la Legislación Sectorial con la específica de Protección de Datos es la que va a regular los tratamientos de datos relativos a salud que se recogen algunos de los tratamientos más importantes en los que se están recogiendo datos relativos a la salud, están los tratamientos relativos a la asistencia sanitaria, vigilancia, epidemiológica, ensayos clínicos, investigación, aparte de otros muchos de naturaleza administrativa, como pueden ser los relacionados con la actividad aseguradora, con sus pensiones por minusvalías y muchísimos más.

Ya para terminar, les voy a relatar cómo afectarían las medidas de seguridad, los datos especialmente protegidos en la regulación específica de protección de datos en la situación española, en la LOPD.

El Reglamento de Medidas de Seguridad que ha citado antes que desarrolla el artículo 9 de la Ley de Protección de Datos, establece tres niveles de seguridad: Básico, medio y alto, y en función de la naturaleza de los datos que son tratados en cada fichero, en cada sistema de información establece una serie de medidas que son de obligado cumplimiento y que son complementarias.

Y así, en concreto, en los ficheros de nivel alto, o sea, en el nivel alto de aplicación de medidas de seguridad se encuentran aquellos tratamientos que contemplan datos especialmente protegidos.

Debe estar implementado un buen sistema de seguridad en la organización, pero además, debe realizarse una auditoría periódica cada dos años para controlar que las medidas de seguridad se apliquen correctamente.

Un tema muy importante. Cuando se está tratando información especialmente protegida fuera de la organización, bien si ese tratamiento se hace mediante un soporte que se ha preparado en la organización para llevarlo a otra entidad o bien cuando esa transmisión se ha hecho a través de una red de telecomunicaciones los datos deben ser cifrados, debe mantenerse un registro de accesos para controlar quiénes acceden a la información, y qué movimientos realizan en la información de los datos especialmente protegidos, y además, debe existir una copia de respaldo para que en caso de una pérdida de información se garantice la recuperación de la misma.

Todo esto, sin perjuicio del respeto al resto de los principios de protección de datos y del cumplimiento del resto de los más sectoriales.

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

Le pediría ahora a la doctora María Marván Laborde su presentación, de quien baste decir por el gran reconocimiento que tiene, que es Comisionada Presidenta del Instituto Federal de Acceso a la Información Pública.

Ponente: María Marván Laborde.

Para continuar con la discusión no abundaré mucho en cuáles son los datos especialmente protegidos, son así definidos en la Legislación española en contraposición a otras legislaciones que determinan o los definen como datos sensibles.

Creo, simplemente, que vale la pena decir que mientras más clara y precisa sea la definición más sencillo será su manejo. Lo que hay en los hechos, es un reconocimiento explícito y claro de que existen algunos datos que necesitan

mayor protección y mejores cuidados por las autoridades que los tienen en todo su manejo a lo largo de todo el proceso que comprenden las leyes de protección de datos personales desde su recolección hasta su transmisión.

Hay, de alguna manera, el acuerdo de, como ya bien decía el doctor Roldán que los datos sensibles, y se empiezan a enumerar una serie de características: origen racial, étnico, características físicas, morales, ideologías, opiniones políticas, convicciones religiosas, filosóficas, estados de salud, estados síquicos, vida sexual y otras análogas.

Y ahí empezamos a tener el problema. Cuando ponemos otras análogas, y hacemos de la definición de los datos que necesitan mayor protección o de los datos sensibles "un cajón de sastre" empezamos a perder claridad y certeza de qué es lo que estamos protegiendo, qué datos estamos protegiendo y por qué necesitan una mayor protección.

Creo que hay una cuestión que es importante hacer clara. Hablamos de condiciones especiales de protección en todas las fases que supone la ley, una Ley de Protección de Datos Personales.

La recolección, el tratamiento, la transmisión y la necesidad de crear o determinar medidas especiales de seguridad, relativas a su custodia y a quién puede y bajo qué circunstancias, tener acceso a estos registros.

¿Qué los hace especiales?

Que alrededor de estos datos tenemos la posibilidad, reconocida o no, de formarnos juicios de valor sobre la calidad de las personas y creo que esa es un cuestión importante.

Los datos sensibles, desde mi perspectiva, o los datos que deben ser especialmente protegidos, son aquéllos que de manera mucho más delicada, tocan la dignidad y la intimidad del ser humano y que por diversas razones nos generan o propician motivos de discriminación o de persecución política, social, racial o religiosa.

En la medida en la que reconozcamos esto creo yo que es importante aceptar que hay una evolución histórica y cultural del concepto de datos sensibles, o bien de lo que tenemos que poner en este cajón de datos especialmente protegidos.

Hay un principio inamovible: Debemos proteger la igualdad del ser humano y asegurar que todo ser humano sea tratado de la misma manera.

Al afirmar que la definición puede variar por la situación histórico cultura del país, tenemos la posibilidad de reconocer que lo que es un dato sensible, porque genera ciertas medidas de discriminación o de no tratamiento en condiciones iguales, en un lugar puede no serlo en otro lugar o en otro tiempo.

Quisiera poner solamente dos ejemplos, que son ilustrativos y que nos llevan a aceptar que esto es una realidad.

En México hasta el año de mil novecientos una parte lógica de las preguntas del censo, era preguntar por la raza de la gente: ¿Usted qué raza es? La gente contestaba: Blanco, indígena, negro, etc.

En 1910 no se levantó el censo, en razón de una gran revolución que tuvimos y a partir de 1920 desaparece la pregunta de raza en el censo.

Hay una política de Estado que, sin necesidad de haber hablado o discutido en ese momento de protección de datos personales, hay una política de Estado que identifica la raza como una razón de discriminación y la saca del censo.

¿Fue bueno o malo sacarlo?

No lo sé. Lo que sí es que la regresaron, pero con base en eufemismos.

Hoy día el censo no me pregunta mí raza, pero sí me pregunta si hablo una lengua indígena. En algunas ocasiones se preguntaba si era yo bilingüe, les aseguro que no estaban preguntando si hablaba yo inglés y español o más

bien si hablaba yo tzotzil y español o nada más tzotzil, por poner un ejemplo.

Hay una evolución histórica que tenemos que atender.

A partir del 11 de septiembre en Estados Unidos, pero en todos los aeropuertos del mundo, la relación religión y raza ha adquirido una preponderancia que no podemos negar.

Si una persona es musulmán, tiene cara de musulmán, tiene cara de árabe, yo puedo presumir o las autoridades de los aeropuertos se dan la libertad de presumir que es un terrorista en potencia, Ahí tenemos cómo claramente hay condiciones históricas que transforman lo sensible de los datos.

Insisto, perdón, tenemos que hablar sobre las características especiales de los datos, no solamente en su custodia, sino en recolección, tratamiento y transmisión de los mismos.

Por la relevancia que ha adquirido en México la discusión acerca del expediente médico, a partir de la aprobación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, centraré mis ejemplos fundamentalmente en este caso, pero creo que son generalizables a muchos ámbitos que tocan los datos sensibles.

Desde luego, parto de la lógica que no podemos reducir la discusión del tratamiento de los datos que requieren protección especial o los datos sensibles a los expedientes médicos, pero en México son un buen ejemplo que nos permite abordar la complejidad de esto.

No existe una sola Ley de Datos Personales en la que no se defina el estado de salud como un dato personal especialmente protegido o sensible. Y por ello me congratulo y lo decía hace rato cuando llegamos y nos saludamos, que la CONAMED esté en esta mesa, esté en esta discusión; créanme que ha sido una preocupación constante del IFAI y mía personal, el pensar que se pueda llegar a aprobar una Ley de Protección de Datos personales en México, que solamente tiene la perspectiva financiera de Hacienda, Banco de México y *Buró de Crédito*, etcétera; dejando de lado las preocupaciones de médicos y pacientes cuando claramente están contemplados en esta lógica.

Hablemos un poquito de la recolección. Quizá lo que primero que tenemos que empezar a definir es, ¿qué debe contener un expediente médico, cómo debe llenarse? Reconocer que existen hospitales de primero, segundo y tercer nivel y que esto nos lleva a complejidades específicas en el expediente y desde luego, en el tratamiento de la persona; reconocer que hay hospitales de investigación y que por la protección de datos personales de una cosa estamos seguros, no queremos que al afirmar que el paciente tiene derecho a conocer su expediente médico en su integridad, esto provoque que el médico deje de escribir.

Si ese es el efecto logrado, algo hicimos mal en el diseño de la normatividad y eso creo que tenemos que tenerlo muy claro. El cuidado en el diseño de las leyes en este momento es verdaderamente crucial.

¿Hasta dónde debe llegar una Ley de Protección de Datos Personales? ¿Cuáles son los principios generales que debe sentar? Y, ¿qué le debe encargar a otras leyes?

Ayer hablamos con toda naturalidad de cómo los datos financieros se transmiten o no en relación a las leyes propias de las instituciones de crédito y demás.

De la misma manera tenemos que lograr una armonización entre la Ley de Protección de Datos Personales con la Ley General de Salud. Y esto me lleva a una extraordinaria ponencia del doctor Roldán hace sólo unas semanas en Chile en el contexto del CLAD (Centro Latinoamericano de Administración para el Desarrollo) que tienen que ver con el proceso de la creación de normas.

No basta con que el sector financiero pueda hacer lobbying. No basta con que la CONAMED pueda hacer lobbying. No basta con que la propia Secretaría de Salud pueda opinar y discutir sobre esto. Tenemos que tomar en cuenta, sin lugar a dudas, la perspectiva del paciente.

En esta medida avanzamos sobre la discusión del expediente médico. Hemos discutido ya en muchos momentos quién tiene derecho, quién es propietario del expediente. Hemos hablado de la necesidad de trascender esta discusión por asegurarle al paciente, cuestión que me parece fundamental, el derecho a ver el expediente médico. No podemos privar al hospital o al médico ni de su responsabilidad ni de su posibilidad de tener y organizar los expedientes médicos.

Y en esta medida quiero yo entrar a un punto que me parece crucial en el tratamiento de estos datos sensibles, en la medida en la que son información sumamente valiosa en el diseño de políticas públicas, así como decía hace un momento quien me precedió en el uso de la palabra.

¿Cómo podemos plantearnos, diseñar políticas públicas de prevención, sin identificar claramente a la población susceptible de contraer, por ejemplo, una enfermedad específica?

Y esto me lleva a la necesidad de usar el dato y manejarlo con toda responsabilidad en una definición territorial. Nadie niega, hoy día, que hay lugares donde se concentra la propensión al cáncer en razón de ciertas contaminaciones y demás y la investigación médica tiene que poder contar con esos datos.

Cómo generar un cerco sanitario si no tenemos una ubicación clara de la población que está siendo afectada por una determinada epidemia.

Las cuestiones raciales y culturales inciden también en esta definición de políticas públicas, es claro que hay ciertas razas donde algunas enfermedades o problemas congénitos son más propensos a suceder que en otros.

Cuestiones socioeconómicas. ¿Quién se atrevería a negar hoy en México que la diabetes tiene una relación muy clara con problemas de desnutrición y problemas donde la población se considera económicamente marginada?

Patrones de la vida sexual. Desde el ejemplo más claro que nos ponían en genética cuando estábamos en primaria, donde fue claro que la hemofilia tenía que ver con los patrones sexuales, permítanme una expresión un poco fuerte, de apareamiento, en la manera en la que se casaban entre los reyes, las cortes, hasta hoy día en cuestiones como la propagación del VIH-SIDA.

Como país yo necesito saber quién es VIH-POSITIVO por qué y esto al mismo tiempo que lo necesito saber no debe dar lugar a la discriminación, ese es el punto delicado del asunto, ni una discriminación laboral, ni una discriminación de cualquier otro tipo.

Me atrevo afirmar, un dato se vuelve sensible cuando su difusión o su mal uso se convierte en motivo de discriminación. Muchos de nosotros hemos tenido la posibilidad de conocer un ejemplo clásico que hubo de resolver la Agencia Española de cadena de supermercados que con base en la fotografía de los solicitantes de empleo determinaron quiénes podían y no podían entrar, gorda, chaparra, fea, tiene cara de mexicana, es decir, aparecieron todos estos datos y con esos elementos discriminaron de la posibilidad de que se consiguiera empleo a un grupo específico de personas.

Los datos o el manejo de los datos en manos del Sector Salud pueden tomar una connotación completamente distinta en manos de las aseguradoras, creo que es importante reconocer que existe una tensión entre los intereses públicos y privados.

Ayer dijimos de manera prácticamente natural, en el seno del trabajo de este Encuentro, que

era válido de alguna manera para el Buró de Crédito manejar los niveles de riesgo y premiar al buen pagador cuando solicita un crédito o quiere comprar algún tipo de mercancía. Si bien este principio puede ser muy claro en este ámbito, probablemente no sea extrapolable sin ton ni son sin tomar en cuenta ciertos principios éticos al ámbito de la salud.

Si las aseguradoras médicas sólo conceden seguro contra enfermedades médicas a quienes no tienen el riesgo de enfermarse, para qué compro un seguro.

Permítanme caricaturizar un poquito, si me hacen un análisis de ADN como condición para darme un seguro y me dicen sólo la podemos asegurar a usted contra tal y cual enfermedad, porque es lo que le podemos asegurar por su ADN, que no va a contraer, como para qué les pago una prima todos los meses o todos los años.

Es decir, son cuestiones que nos llevan realmente a tratar de entender y manejar la complejidad que tiene el manejo, perdón, la redundancia, de estos datos sensibles.

Cuando hablamos de datos especialmente protegidos, normalmente se incluye en las legislaciones de datos personales la necesidad de disociarlos, disociarlos de quién, del dueño de estos datos.

Y aquí permítanme también problematizar un poco. ¿Cuándo y cómo debemos disociarlos? Si un expediente médico va a ser utilizado para la investigación, me queda claro que debemos de disociarlo del nombre y rostro del paciente a fin de que éste no pueda ser identificado y en última instancia discriminado por su condición de salud, pero al mismo tiempo tenemos que permitir al Sector Salud, a quien se dedica a la investigación médica, darle seguimiento a las personas desde que nacen hasta que mueren y todavía más, aún yendo hacia sus antecesores o descendientes.

Resulta una verdad de Perogrullo afirmar que problemas de desnutrición en la infancia tienen consecuencias claras en mi estado de salud en la vida adulta. Que la tendencia familiar a la diabetes o el cáncer puede predisponer a mis hijos a tener cáncer o diabetes.

Sin embargo, si esto va a ser razón o motivo para que no se me dé un seguro, para que no se me trate en un hospital, para que no se me contrate, tenemos que tener precisamente un cuidado en donde la ética atraviesa siempre y permanentemente este tipo de manejos.

Los datos especialmente protegidos requieren una reflexión sería de las condiciones de la transmisión. ¿Quién y bajo qué circunstancias tienen derechos a tenerlos y/o recibirlos? ¿Cuáles son las medidas de seguridad electrónica, desde luego, y no nada más electrónica de almacenamiento y custodia de los mismos?

Y aquí venimos a otro punto que en la discusión de las leyes de datos personales es crucial: ¿Qué tipo de consentimiento requiere el manejo de estos datos que ya hemos definido como especiales?

Es claro que necesitamos un consentimiento expreso, firmado y claro que cubra todas y cada una de las partes del proceso. Su recolección, su tratamiento y su transmisión. No es nada más el permiso cuando voy a recolectar los datos, no es nada más el permiso para poderlos manejar y tratar, participar de una investigación o transmitirlos. Cada una de las fases va requiriendo consentimientos expresos, que tienen que estar claramente enmarcados en la ley, de tal manera que sean una realidad operable, pero que garanticen al individuo esta protección de sus datos.

Parto, desde luego, del derecho a saber. Cuando ingreso, por ejemplo, a un hospital-escuela, yo sé que por definición mis datos pueden ser utilizados para la investigación. No es nada más saberlo por definición. Creo que lo menos que merece una persona que es paciente de un hospital-escuela, es que se le advierta y pida su consentimiento de que su expediente médico será parte de una investigación, y asegurarme

que tenga yo este conocimiento. Es decir, en última instancia las leyes de protección de datos personales nos llevan a nosotros, como individuos, a adquirir conciencia de que somos cajas completas de información, y que el manejo de estos datos debe hacerse con todo el respecto a mi dignidad de persona, y en beneficio también individual y también social.

Por eso creo que es importante poner el ejemplo de la importancia del manejo de los datos sensibles en el diseño de políticas públicas.

Tenemos que partir de reconocer en el manejo de estos datos de la capacidad de autodeterminación del ser humano, que en este caso específico nos lleva a afirmar la autonomía del paciente, y a dejar atrás prácticas paternalistas, que nos llevan a suponer que existen seres humanos, hombres y mujeres, que deben o no pueden ser tratados como adultos. O dicho de otra manera, que los tenemos que tratar como eternos menores de edad.

Hablar de protección de datos personales, hablar de tomar conciencia como persona que tengo estos derechos, es en última instancia un reconocimiento de la libertad humana, y un reconocimiento de que todo ser humano tiene y debe protegerse su capacidad de razonar y de escoger.

Creo que ésta es, en alguna medida, la esencia del tratamiento especial que le debemos dar a los datos personales que nos llevan a la necesidad de una definición clara, de previsiones normativas cumplibles en todas las fases del procesos: recolección, tratamiento, transmisión, almacenamiento de datos y acceso a los archivos de los mismos y, desde luego, como ya decía también el doctor Roldán, a sanciones específicas que realmente sean capaces de disuadir al trasgresor.

El día de ayer conversábamos en la cena con el doctor Piñar Mañas. Hay compañías españolas que prevén en su presupuesto hasta 6 millones de euros, para pagar en multas por el mal tratamiento de datos.

¿Qué quiere decir? Que ellos ya hicieron un cálculo que pueden ganar, por lo menos 6 millones de euros más uno, en caso de violar la ley. Esas son las cosas que tenemos que tomar en cuenta en el diseño de una norma y por eso, créanme, me congratulo mucho que estén en la mesa con nosotros.

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

Quiero decirle que en el Sector Salud y particularmente en la Comisión Nacional de Arbitraje Médico, reconocemos este interés no solamente jurídico, legal, de entrar al estudio del tema, sino un interés legítimo que en este momento se reconoce con sus palabras, pues se nota que el Instituto de Acceso a la Información, su Presidenta y el resto de los señores Comisionados tienen este interés en abordar el tema, para beneficio no de las instituciones, sino concretamente, como usted lo señalaba, de los propios pacientes.

Así que muchas gracias por habernos invitado.

Ponente: Fabrique Gallegos.

Quiero aclarar que vengo en representación de Abraham Sotelo Nava; soy Director General en la Unidad de Gobierno Electrónico y Política de Tecnología de la Información. Me dedico a la operación de todos los sistemas electrónicos que ofrece la Secretaría de la Función Pública.

Primero explicaré un poco sobre lo que estamos haciendo en medidas de seguridad y en especial con los datos especialmente protegidos.

Los voy a sacar un poco de contexto en el sentido de que no voy a hablar sobre expedientes médicos, voy a hablar de lo que estamos haciendo en el ámbito de la tecnología.

La Secretaría de la Función Pública, antiguamente la Secretaría de la Contraloría y Desarrollo Administrativo, ha cambiado de funciones a partir de enero de 2004; es decir, ha

tenido nuevas atribuciones y estas atribuciones involucran precisamente a la Unidad de Gobierno Electrónico y Política de Tecnología de la Información, a generar esto: Política en Tecnología.

Para la presente administración el tema tecnológico es de gran prioridad, es una alta prioridad y, por lo tanto, los resultados que nosotros hemos ofrecido y realizado en el tema tecnológico, nos han generado que nuestro sentir, nuestro ser y nuestro saber es ahora el ciudadano. Ese es nuestro centro de atención, es nuestro centro de acción.

Por lo tanto, al tener, como nosotros, al ciudadano en medio, queremos recuperar esa confianza perdida del ciudadano con su gobierno. Es decir que el ciudadano tenga un gobierno que funcione como todos queremos; un gobierno el cual sea eficiente, el cual sea eficaz, el que sea oportuno, el que sea seguro y, por lo tanto, se ha generado una estrategia general, la estrategia de buena agenda, de buen gobierno, que comprende diferentes líneas de acción, en donde le estamos ofreciendo al ciudadano diferentes acciones en materia sobre su gobierno, que tenga un gobierno que cueste menos, de calidad, profesional, digital, con mejora regulatoria, honesto y transparente.

En la utilización de la tecnología, en la utilización de la mejora regulatoria, es precisamente ahí donde la seguridad que hemos dado a los sistemas que producimos juega un papel relevante.

La aplicación y el uso de la tecnología de la información, si bien nos ofrece ventajas para que el ciudadano tenga una calidad de vida mejor, para que el ciudadano tenga facilidades de interacción entre gobierno, sus particulares, las empresas y el propio gobierno, que tenga un mejor desarrollo social y económico.

También la tecnología en una utilización incorrecta puede convertirse en una amenaza. Cuántos de nosotros no hemos utilizado los cajeros automáticos y sentimos amenaza cuando utilizamos un medio electrónico, el que nos pueda dar el dinero correcto que estamos solicitando; cuántos de nosotros también consultamos o hacemos una transacción vía Internet o recuperamos nuestra Curp a través de Tramitanet.

Existe una gran diversidad de trámites y servicios que ahora se ofrecen a través de estos medios y que pueden resultar en una mala utilización, puede resultar una amenaza para el propio usuario, puede formar una manera de exclusión o tener alguna condición de incertidumbre o de riesgo por la propia transacción electrónica que se esté realizando.

Nosotros creemos en principios básicos en la protección de datos, sean datos personales o sean datos no personales.

Uno es el principio de legalidad. Tener los datos precisamente en el ámbito legal que son requeridos, no pedir más, no pedir menos simplemente los que legalmente podemos pedir, los datos que sean de calidad, es decir, no contar con información que sea basura o que sea incorrecta, que sea impropia.

Uso y destino de la información. Precisamente saber cómo se van a utilizar estos datos y dónde van a estar almacenados, es un principio muy importante.

La seguridad que implica diferentes tipos de seguridad, llámese física, lógica y, la custodia y consentimiento para la transmisión de datos. Es decir, hacer una transacción electrónica tenemos que tener el consentimiento de ambas partes y de esa manera van a poder comunicarse y serán válidas sus transacciones.

En el ámbito de la custodia se han generado diferentes acuerdos en donde la Secretaría de la Función Pública tiene en custodia, por ejemplo, bases de datos de servidores públicos conteniendo información muy sensible en donde podemos definir datos que son personales, aquellos que relacionan a la identificación de la persona y aquellos también que comprenden su

información en archivos, es decir, la que tiene relacionada con esa misma persona. Pero aún así existen datos que no necesariamente son personales y que requieren ser también especialmente protegidos.

La Secretaría de la Función Pública ha generado diferente tipo de seguridad y política para la utilización correcta de estos datos.

La política de la seguridad física. En nuestras oficinas seguridad física implica tener accesos restringidos en nuestras propias instalaciones, custodia de los archivos físicos que podemos tener, circuitos cerrados de televisión en donde podemos verificar exactamente las personas que estamos autorizadas a trabajar en el piso asociado a nuestra unidad.

La seguridad lógica que conlleva a la utilización de registros electrónicos que nos permitan la entrada electrónica a nuestras instalaciones.

El acceso a los propios sistemas que implican también una seguridad lógica, implican una seguridad desde el punto de vista de la utilización de las bases de datos, de los roles que juegan los que custodian las bases de datos y los roles que juegan quienes hacen uso de estas bases de datos.

Así también la utilización del correo electrónico en el sentido de no volverse un distribuidor de información, tal vez confidencial. También la seguridad en redes, proteger ciertos segmentos de transmisión de datos por los cuales no pueden transitar los mismos para los cuales la Secretaría de la Función Pública ha generado este tipo de políticas de identificación y de autentificación, utilizando también mecanismos como la firma electrónica, la firma electrónica avanzada, en donde la Secretaría de la Función Pública a través de diferentes acuerdos normativos hemos generado este mecanismo que nos da una confidencialidad de autenticidad de los documentos electrónicos que estamos utilizando, entiendo por autenticidad aquellos documentos en donde podemos ser e identificar al autor del propio y también la confidencialidad guardando el acceso al propio documento y restringirlo a quien únicamente pueden verlo.

Aunado a ambas partes, la confidencialidad y la autenticidad nos da para nosotros lo que utilizamos ahora que es la firma electrónica y la firma electrónica avanzada, utilizado infraestructura de llave pública y llave privada.

Con ello hemos generado diferentes sistemas, como es el sistema Compra-Net, que es el sistema para las compras del Estado, en donde utilizamos este tipo de mecanismos donde protegemos datos sensibles que no necesariamente son personales. También tienen que ver con datos en donde una transacción puede llevar a cabo algo en negocio, es decir, algo en dinero, aquellos proveedores y contratistas que quieran contratar con el Estado pueden enviar sus ofertas a través de este sistema y podrán ser ganadores, tal vez, de un contrato de un concurso; por lo tanto, la protección de sus transacciones es sumamente importante, así como los datos que contienen cada una de esas transacciones, no pueden ser revisadas por nadie más, solamente en tiempo y forma que está adecuado o realizado para la utilización de este sistema.

También este sistema ha sido auditado por el Banco Mundial, precisamente en el aspecto de seguridad.

Tres ejemplos más donde utilizamos protección de datos muy importantes: sistema de Declaranet, que nos permite a nosotros, servidores públicos, presentar nuestras declaraciones patrimoniales; es decir, nosotros como servidores públicos tenemos la obligación de presentar cuánto ganamos, qué propiedades tenemos (bienes muebles, cuentas bancarias) que le asegura poder identificar al gobierno con lo que contamos en el ejercicio de nuestro servicio.

Existe otra iniciativa como es el sistema@campus donde nos permite identificarnos a través de estas llaves públicas y privadas y poder tener acceso como servidores públicos a capacitación en línea.

También existe otro sistema, el Sistema RUPA, que es el Registro Único de Personas Acreditadas que nos permite acreditar la personalidad jurídica de una empresa que quiere hacer trámites y servicios con el Gobierno Federal y cuenta con toda su información y es válida en todas las dependencias; es decir, su información puede ser visible por los interesados para realizar trámites y servicios en las demás dependencias.

Con esto espero haber dado un panorama general de lo que estamos haciendo en la Secretaría de la Función Pública y especialmente en los productos y servicios que estamos ofreciendo a la ciudadanía.

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

A continuación le pediría al doctor Enrique Domville, quien es médico egresado de la Universidad Nacional Autónoma de México, que tiene una amplia experiencia y trayectoria de 25 años en diversas instituciones del Sector Salud.

Fue asesor en tecnología de la información del expediente clínico y actualmente es asesor del Subdirector General Médico del ISSSTE.

Ponente: Enrique Domville Domville.

Los datos especialmente protegidos. En este momento estamos adoptando un lenguaje, pero en realidad estos datos a nosotros nos los enseñaron en la facultad que teníamos que protegerlos y teníamos materias como sería la Introducción a la Clínica, donde nos hicieron hincapié de cómo obtener la información para ayudar a nuestro paciente, por supuesto que esa información tiene que ver con todos los datos que pueda el paciente darnos para poderle ayudar.

¿Cómo se guarda el expediente? Nosotros tenemos en el país actualizaciones del siglo XIX, del siglo XX, siglo XXI, estamos en una época de transición, donde estamos cambiando del papel al óptico, al electrónico. En este momento decir que todo el material está debidamente protegido en todo el país, sería redundar en una necedad y error.

Los Usuarios:
¿Quiénes son los que pueden acceder al tipo de información que nosotros manejamos? ¿El personal del hospital? Me atrevo a decir no legal, sino judicial, porque habitualmente se requiere una orden para la entrega de un expediente, y se puede usar desde el punto de vista comercial.

¿Qué es lo importante? El respaldo. ¿Por qué necesitamos respaldo? Porque hemos visto recientemente, en diciembre del año pasado un tsunami que acabó con información médica en todo el Sureste Asiático. Tenemos un temblor del 85. Tenemos recientemente huracanes en la zona sur del país. La protección no nada más va contra el mal uso de esa posible información, sino a la protección, tiene que ver con guarda, tiene que ver con el poder seguir ayudando a aquel que lo necesita, y por lo tanto su información, porque es muy difícil acordarnos de todo. Tal vez el paciente se acuerde de algunos detalles, pero para eso utilizamos el expediente, precisamente para remarcar y recalcar todos aquellos avances o diagnósticos o bien estudios que se hayan hecho.

¿Cuáles son los peligros? Los peligros son, la consulta fraudulenta. Siempre hay alguien que quiere obtener algo, además de su salud. Alguien quiere utilizar la información para otros fines, no para los que fue creado. A esto nosotros le tenemos que denominar de alguna manera consulta fraudulenta.

Tenemos la sustracción de esa información, se roban los expedientes para fines de personal y tenemos los desastres que ya hacia mención.

La empresa por no decir el sistema médico, que puede ser desde el individuo hasta una institución privada o pública, y el usuario son los responsables, porque ambos tienen derechos y obligaciones.

Mencionaba la doctora hace un momento sobre la importancia de lo que sería el consentimiento informado. De acuerdo a la regulación de nuestro país nosotros utilizamos lo que es el consentimiento informado. En este momento no se practica ninguna circunstancia de orden médico si no está con firma autógrafa en el expediente el procedimiento o lo que se le va a hacer al paciente. Siempre está por escrito con la autorización.

La información tiene un flujo. Tenemos dos tipos de información, una que proviene del hospital y otra que provendría de una delegación.

La delegación tiene varios tipos de unidades. Las unidades podrían ser de primer nivel, podrían ser clínicas hospitales u hospitales generales. Y tienen guarderías, oficinas administrativas, velatorios, almacenes. Todos estos manejan información privilegiada, información que puede ser de uso comercial, esta información privilegiada tenemos que custodiarla.

Pero la más importante es la que se genera tanto en las unidades médicas como en las guarderías.

Ahora, acuérdense ustedes que nosotros tenemos la posibilidad de la dualidad. En determinado momento podemos ser custodios de la información y en otro momento estamos proporcionando la información, porque requerimos nosotros del tratamiento médico.

En los hospitales regionales hay que ver cómo está su estructura, el abasto, el personal, los accesos. En personal tenemos fichas de identificación del personal, que además pueden ser derechohabientes de los propios hospitales. Por lo tanto, aquí se maneja el sistema de que tenemos archivos separados y tenemos varios archivos.

Ahora, cuando tratamos de evaluar la estructura aquí vamos a ver los daños que ocasionó y esos daños nos llevan a verificar la información, si es un daño interno o es un daño externo.

Si es un daño interno tenemos que evaluar si puede seguir operando. Esto quiere decir que si tenemos los recursos para seguir atendiendo a la gente que lo requiere, ya sea a nuestros derechohabientes, población abierta o a nuestro mismo personal, y hay que evaluar los por cientos. Todo esto es información que puede ser privilegiada, aunque en este momento no son datos personales, pero todo esto va influir sobre los datos personales, porque va ser la manera con lo que vamos a poder o no poder hacer nuestras acciones y se tiene que plasmar en un documento, que es el expediente clínico.

Ahora, si el daño es externo poco podemos hacer, pero tenemos que ubicarnos en el lugar de sitio.

Nosotros necesitamos saber qué abasto tenemos. ¿Por qué? Pues porque esto se va reflejar otra vez en le expediente. Nosotros vamos a saber si le podemos dar agua, si le podemos dar medicamentos, si los tenemos o no los tenemos. Todas estas acciones se reflejan o se van a reflejar sobre los datos especialmente protegidos del expediente clínico.

El personal. En un desastre tenemos que saber qué personal estaba, necesitamos saber quiénes estaban y si les ocurrió algo en nuestras instalaciones o si no llegaron a nuestras instalaciones y, por lo tanto, si están ausentes de las áreas.

¿Cómo son los accesos?

El tipo de atención. A cada uno de éstos que le estamos dando atención, nosotros tenemos que hacer un registro de la atención que estamos dando y, por lo tanto, se vuelven datos especialmente protegidos, pero estos datos se toman en circunstancias muy especiales, porque estamos frente a un fenómeno.

La organización. Esta organización, para obtener los datos, guardar los datos y conservarlos durante el desastre, pues es un reto que no está regulado, es un reto que hay que pensar y que hay que trabajar mucho.

¿Con qué frecuencia vamos a actualizar estos datos? ¿Cada seis horas, cada ocho horas, cada 12 horas?

Pues va depender de la organización previa al desastre que tengamos, para el manejo de este tipo de información.

La información en hospitales. Pues toda esta información va estar en relación con el expediente clínico; el nombre del hospital, en fin, etc., la fecha de inauguración, las historias, las anécdotas, la capacidad física de un hospital, el número de camas, consultorios, urgencias. Todo esto influye sobre el documento que estamos hablando, que está especialmente protegido.

El número de camas, consultorios de urgencia, consultorios de gineco-obstetricia para saber, por ejemplo, la capacidad resolutiva. Si nosotros vemos dos pacientes por hora y tenemos un consultorio, pues no vamos a poder ver más de dos pacientes por hora. Los quirófanos de la misma manera para ver su capacidad.

Todos estos auxiliares de diagnóstico son parte importante de lo que contiene el expediente clínico, ya que estos datos hablan de una parte del tratamiento o hablan en especial de algunas terapias que se usaron, como por ejemplo en el banco de sangre, si se ha transfundido, si no se ha transfundido.

Y habitualmente todas éstas traen el diagnóstico presuncional.

El archivo: El número de expedientes que manejamos. En promedio es uno por población derechohabiente, si el ISSSTE tiene 10 millones de derechohabientes, pues vamos a tener teóricamente 10 millones de expedientes, pero no es así. Cada nivel de atención tiene su propio expediente, entonces estamos hablando de la posibilidad de 30 millones de expedientes, mas si fue atendido en otras unidades, aparte, que no le correspondía, entonces estamos hablando de muchísimos datos, de millones de datos.

Estamos haciendo 90 millones de acciones médicas por año. Estos 90 millones de acciones médicas se reflejan en un expediente y en este reflejo estamos hablando de que hay que guardar esos 90 millones de acciones, de alguna manera, para que no tengan un mal uso y puedan hacerse para lo que son, para ayudar a nuestros pacientes.

Ahora bien, antes de llegar a decir que hay una regulación o que estamos en proceso de, nosotros tenemos que llamar a los responsables y decirles, el contexto ha cambiado. Nosotros en este momento vamos a hacer conciencia de los millones de datos que manejamos, que necesitan ser salvaguardados. Por lo tanto, debe de existir un cuerpo colegiado de expertos que dé asesoría, antes de auditoría, primero tiene que dar asesoría para formar y, posteriormente certificar el cumplimiento del mismo. Yo le llamaría asesoría y certificación en lugar de auditoría.

Moderador: Agustín Ramírez Ramírez. Subcomisionado Jurídico, CONAMED.

Cédric Laurant, voy a señalar brevemente su currículum, es Consejero de Políticas de EPIC, centrado en temas de privacidad internacional y políticas comparativas y aspectos legales de los regímenes europeos y estadounidense; su trabajo reciente se ha enfocado en los ficheros de viajeros aéreos, vídeo vigilancias, tecnologías de identificación de radio frecuencia, en la negociación de las directrices en privacidad, de la APEC y, en el tema de vigilancia electrónica gubernamental; es master en Derecho por la Escuela de Derecho de la Universidad de Columbia.

Ponente: Cédric Laurant.

Voy a explicar principalmente la situación en los Estados Unidos, el concepto por sí mismo no existe. Lo que sucede en los Estados Unidos son diversas regulaciones que cubren tipos específicos de información y en las legislaciones se menciona una referencia donde existen datos sensibles.

Los datos sensibles son algo que se refiere no sólo a muchas cosas, sino a uno muy importante que es la dignidad, que cuando se utiliza de una manera adecuada por las autoridades se llaman realmente datos sensibles.

Entonces, al formar este concepto nosotros podemos ver que estamos rastreando y perfilando un desafío hacia la sensibilidad de protección de datos o la protección de datos sensibles.

Recientemente y posterior al huracán se publicaron y las autoridades empezaron a decir que se podían identificar mejor las tarjetas de identidad, así que ahora en los Estados Unidos existe un gran debate sobre si estas investigaciones son desafiantes o no, y si se puede dar la aplicación de la ley con las agencias gubernamentales que están tratando con esta situación de emergencia.

Yo me enfoco en tres casos principales: El primero, es la supervisión de los niños; la segunda, es la de los empleados en un lugar de trabajo y la tercera de las situaciones importantes.

En el primer caso la vigilancia de los niños tiene un tipo de datos que se refieren a la educación y hacia dónde van los niños desde su escuela o su kindergarten para ver qué es lo que se identifica con respecto a los menores.

Esto fue algo reciente en los Estados Unidos, por ejemplo, en los parques de diversiones como Disneylandia, Six Flags, etc., y se están pidiendo huellas digitales en todos los patrones que incluyen niños.

Si este fuera el caso en la Unión Europea, si fuera una situación de protección de datos entonces estaría prohibida en los Estados Unidos puesto que no hay una situación de datos, de protección de datos unánime, ya que esta recolección de datos no es permitida. Las compañías tienen el derecho de recolectar datos, pero no siempre huellas digitales, lo interesante en este caso es que el propósito es muy sensible, porque la mayoría de las personas en los Estados Unidos creen que las huellas digitales son datos realmente sensibles, la razón para recopilar esto es que evita que las personas utilicen la identificación de alguna otra persona, pero el propósito mismo no es proporcional el tipo de datos y la sensibilidad de esta recopilación de los datos.

Este problema de protección de datos es que no existe una proporcionalidad, la recolección de huellas digitales con el propósito de asegurar los datos y de la persona que necesita utilizar esto de la misma manera, de una manera legal excede esta proporcionalidad.

Otra situación que me interesó es que el 99.9 por ciento de estas situaciones no se dan cuenta de que cuando se les pedía que hicieran una firma, que pusieran sus dos dedos, el índice y el medio, la mayoría de ellos no se daban cuenta de que en realidad estaban proporcionando sus huellas digitales.

Lo que sucede con estos datos es que los propósitos que se están generando se utilizan posteriormente por las autoridades, entonces, la tercera y la más importante es que las personas no dan un consentimiento explícito para que se utilicen estos datos o las huellas digitales como hemos estado diciendo.

Otro caso interesante que se llevó a cabo a principio de este año, se presentó en California, era un rastreo de niños con diferentes implicaciones. Los obligaban a utilizar unos como delantales, donde estaban ocultos estos arsenales, y les podían, les decían que era situación de manejar mejor a estos niños. Y aquí podemos ver que esta situación generaba el propósito que estábamos viendo que había grandes problemas, y que estaban manejando estos datos tan sensibles a su entender, registrando toda la situación que estaba generando los niños en cualquier momento.

La situación de la protección de datos en Estados Unidos principalmente tiene un alcance de la dignidad de los seres humanos, incluso aquí que

estamos hablando de niños, y son niños que no sacan una tarjeta de identidad, ni existe una proporcionalidad entre el tipo de datos que se están utilizando para medir esto y el propósito que éstos tienen.

También se refiere a la implicación del consentimiento y de la transparencia. Esto con una implicación que nos da una situación de los datos y la tecnología, es un propósito que se inicia para tratar a los seres humanos, para rastrearlos como vegetales, como latas o como situaciones de embarque.

También puede tener un impacto. ¿Qué tan fácilmente podría darse que esos niños fueran discriminados en cierta instancia, debido a que esa información que está contenida aquí se puede manejar no solamente por los que se les requirió, sino también por cualquier persona que tenga acceso a esta información y por todas las personas que puedan entrar en contacto con los niños, y podrían leer la información de este niño?

Otro caso interesante es la supervisión o la vigilancia en el lugar de trabajo, en el uso de pactos, de cartas o de tarjetas de identidad.

El uso de tarjetas listas, de tarjetas que se utilizan para dar un acceso, para Internet específico en el lugar de trabajo. Estas tarjetas astutas a veces son realmente seguras.

Pero en general no tiene sentido, por ejemplo, en los hospitales o en algún otro tipo de instalación tampoco tiene sentido si se hace este tipo de situación en todo el ambiente de trabajo.

También eso ha sido terminado por la investigación que se ha dado en el gobierno, que se investiga a ciertas compañías, para entender de una mejor forma cómo estas compañías podrían recopilar o utilizar este tipo de tarjetas astutas y utilizarlas como una referencia futura para definir este tipo de personas que ellos contrataban.

La mayoría de los registros estaban en una forma personal y el empleado podía ser rastreado, podía ser encontrado por sus patrones en cualquier lugar, en cualquier posibilidad o en cualquier región en que éste estuviera; en grupo, en el lugar en que se localizara, con quién se estuviera socializando, con quien se estuviera relacionando, con otros empleados.

Por lo tanto, también es interesante al definir esto, que solamente una de las compañas, dadas las cláusulas específicas y escritas, en las que ellos lo autorizaban, donde no se utilizara este tipo de datos en contra de las personas que estaban siendo empleadas y de unas pólizas especificando cómo más adelante estos datos solamente se utilizarían para el momento en que se estaban contratando.

Así es de que uno de los asuntos más importantes de protección de datos es que esas tarjetas, aunque originalmente se utilizaban primero para abrir puertas, digámoslo así, generaron una gran cantidad de datos que se recopilaban posteriormente con esos propósitos y eran una situación diferente, puesto que en lugar de beneficiar los perjudicaba, a pesar de que se pudieran considerar como situaciones de seguridad.

Y entonces aquí podemos ver que el uso de este sistema de rastreo, que modifica el equilibrio entre la conveniencia personal, la seguridad en el lugar del trabajo y la privacidad, nos lleva a una pérdida de seguridad privada.

En los Estados Unidos esto no se considera dentro de los derechos humanos, puesto que se está hablando de la Constitución, puesto que se considera como valor, que se pone en situación de la supervivencia en el lugar de trabajo. La seguridad y la conveniencia personal, en este caso en particular, son de un uso y un valor de una conveniencia personal, a pesar de que esté atentando contra la seguridad y contra los valores individuales.

La tercera área de supervisión era la situación de poder tener un chip subcutáneo, que muchas compañías estaban utilizando para ayudar a los paramédicos y a los doctores para poder tener en caso de que el paciente permaneciese inconsciente y no pueda dar su información o su historial médico.

Es muy poco probable, es muy poco conveniente que se promueva una tecnología que permanentemente ate al ser humano con un chip, una vez que desde aquí ya no va a tener esta situación de privacidad y de tranquilidad que pudiera lograr.

También se propuso un marco para regular esta situación y pensamos que lo que podríamos hacer con este asunto y los generales, sería identificar y no ocultar de una manera personal la identificación personal, pero si se pudiera encontrar podemos decir que podría ser una situación no permanente, pero que sí se relacionara con el individuo en específico.

Esto debería ser una incertidumbre. Aquí el caso con los pacientes que están etiquetados por este tipo de chips, por seguridades de su privacidad puesto que se está afectando su identidad. También sería el caso del uso de este tipo de tarjetas que están permanentemente ligadas a los individuos, esto representa a las personas que están originando esta identificación. Estaría prohibido este tipo de chip.

Como conclusión general yo quisiera proponerles que pensaran y consideraran. En los Estados Unidos lo que sucede es que la mayoría de las personas piensan en los riesgos, en los tipos de datos específicos, en los duplicados, cuando estamos hablando de los individuos y en general es un marco que el legislador y los que hacen la política deben de valorar cómo estos sectores específicos deberían de ser interrelacionados o cómo estos datos deberían de ser recopilados.

Y también siempre deben enfocarse hacia una situación de una privacidad en general, que conforma no obtener o poseer los datos a través de la tecnología, sino de una tecnología futura y de una protección de este tipo de datos. Estos ejemplos, yo les quiero demostrar que las compañías empiezan a pensar en la tecnología y en el interés de tener una base de datos comprensiva total.

Y por ejemplo esto afecta a Microsoft porque tienen asuntos de privacidad, problemas con su privacidad. También que vean esta situación de que estos tres factores claves se deben apoyar con estas compañías y deben de responder de una manera legislativa.

Primero la conclusión potencial con los congéneres de otros tipos de datos que se podrían cubrir. También el incremento de poder tener más confrontación con la recolección de datos personales que pueda afectar una situación y también incrementar los códigos de acceso para poder mejorar la seguridad.

Y también esto debería realmente hacerse, sobre todo en el trabajo de Microsoft. Han propuesto también un marco específicamente con respecto a la información que influye en los requisitos de obtener un consenso explícito por parte del consumidor para que entre en vigor este año.

La protección de los datos personales en los Estados de la República Mexicana

Mesa 8

Moderador: María Marván Laborde. Comisionada Presidenta del IFAI.

Tengo el agrado de coordinar esta mesa de protección de datos personales y la legislación que está realmente vigente en algunos de los estados de la República.

Ponente: Ramona Carbajal Cárdenas. Comisionada Presidenta de Acceso a la Información Pública del Estado de Colima.

A todos ustedes les agradezco el favor de su atención y las consideraciones para el contenido de mi exposición, respecto de un tema de singular relevancia y actualidad, como lo es el tratamiento de los datos personales en la legislaciones de los diversos Estados de la República, situándome desde luego en mi estado, Colima, uno de los estados más pequeños de la República que está enclavado en el Occidente mexicano.

Desde el año de 1977 el Constituyente de la República abrió en nuestro país la posibilidad jurídica de que los mexicanos tuviésemos acceso a la información pública al reformar el artículo Sexto, para establecer que el derecho a la información será garantizado por el Estado.

No obstante, dicho imperativo, cuya inclusión en nuestra Carta Magna generó un derecho social, fue hasta hace aproximadamente tres años que se aprobó la Ley Federal de Acceso a la Información Pública Gubernamental y con posterioridad la mayoría de los Estados de la República se han incorporado a esta dinámica con las leyes locales correspondientes.

Paralelamente a la necesidad de la transparencia, a lo público, surge el requerimiento de proteger a las personas del uso indiscriminado y potencialmente lesivo de sus datos personales.

Algunos de esos factores inciden en los siguientes tópicos: Las implicaciones que pudieran generarse por las inadecuadas interpretaciones de las leyes de acceso a la información. El avance tecnológico en materia de informática y de redes de cómputo.

En esas condiciones y ante la clara necesidad de brindar al ciudadano una protección adecuada contra el posible mal uso de la información que le concierne, se motivó que el Ejecutivo del estado enviara una Iniciativa de ley que el Congreso local aprobó y que contiene la protección de datos personales del estado de Colima, en vigor desde el 22 de junio del 2003

Los objetivos de esta ley son similares a los que determinan para el Hábeas data. Tratando de hacer breve esto citaré algunos de los siguientes derechos: *El ciudadano tiene derecho a conocer de su inclusión en los bancos de datos o registros. Tener acceso a la información que sobre él conste en los bancos de datos o registros, y actualizar o corregir, en su caso, la información que sobre él obre en dichos bancos, y muy importante conocer también los fines para los que se va a utilizar esa información*.

Que se garantice la confidencialidad de determinada información obtenida legalmente, para evitar el conocimiento de terceras personas. Ya se ha dicho mucho en estos días, se necesita el consentimiento del dueño de los datos para que lo tengan terceras personas. *Y que se garantice la supresión de la información que sobre él se encuentre en poder de terceros y que se refiera a cuestiones personales*.

Todos estos derechos convergen en un propósito inmediato y fundamental, que es el de proteger el derecho a la privacidad del individuo, derivado del mandato consignado en la fracción sexta del artículo Primero de la Constitución del Estado de Colima, el cual establece que las autoridades del estado velarán por la defensa de los derechos humanos e instituirán los medios adecuados para su salvaguarda.

La Ley de Protección de Datos Personales en Colima, es entonces uno de los medios que el estado instituyó para el propósito que acabamos de citar.

Dentro de los puntos que motivaron la expedición de la Ley en comento citaré nada más un caso, para hacerlo más breve, *la necesidad de proteger la privacidad de las personas como uno de los derechos fundamentales del hombre*.

La Ley en comento consta de 23 artículos en seis capítulos. El Primer Capítulo nos trata el tema de las disposiciones generales.

El Segundo Capítulo nos habla de los datos personales.

El Tercer Capítulo nos trata de la creación y de la protección de dichos datos.

El cuarto capítulo se dedica al tema de los archivos, muy importante.

El quinto capítulo de la Comisión, pero de Acceso a la Información Pública, que es la encargada de tutelar la Ley de Protección de Datos Personales.

Y el último tema tratado en esos seis capítulos es precisamente lo que se refiere a las infracciones y a las sanciones. En un primer plano se precisa que la ley será aplicable dentro del estado de Colima a los datos de carácter personal, que serán registrados en los sectores tanto público como privado en cualquier soporte físico que nos permita el tratamiento de los datos.

Y el propio texto jurídico señala, como datos personales, *aquellos que de manera directa o indirecta puedan conectarse con una persona específica*. De aquí surge la diversidad de la ley que contempla en cuanto al tratamiento de datos personales dos vertientes: Las que maneja el sector público y las que maneja, por supuesto, el sector privado.

La ley establece disposiciones comunes en el manejo de datos de carácter personal, las que deben ser observadas por las dependencias del sector público y, desde luego, como personas físicas y morales que deben manejarse en el sector privado.

El artículo Cuarto de la propia Ley de Protección de Datos señala que para el manejo de los datos de carácter personal, se seguirán los siguientes principios: Primero, los datos que se obtengan deben ser adecuados, pertinentes y no excesivos. También señala que deben usarse esos datos expresamente para los fines que fueron obtenidos y que deben ser correctos y actualizados. Y además, cosa muy importante,

que se deben de obtener por medios lícitos, no se vale que sea de manera fraudulenta o que sea de manera ilegal. Y para obtenernos se debe de informar al interesado de su existencia y del fin del archivo.

Para el tratamiento de los datos personales debe obtenerse el consentimiento explícito e inequívoco del dueño de los datos y también se le tendrá que enterar quién es la persona responsable de vigilar y de cuidar dichos archivos.

En el sector público, la verdad nos maravillamos de la cantidad de datos personas que tienen de nosotros, que a la mejor ni nosotros sabemos tanto. Saben perfectamente, nos tienen bien vigilados, qué hoteles nos gusta, cuáles son los restaurantes de nuestra frecuencia.

Encontramos datos personales en los padrones electorales, en los padrones de catastro, de contribuyentes, de instituciones del sector social, por ejemplo, ISSSTE, el Seguro Social, en Educación, en la Secretaría de Hacienda, en cuanto algunas personas se hicieron acreedores a beneficiarse por algún programa oficial, allí están todas nuestras bases de datos. Esto es por citar algunas fuentes.

Por esta razón en la misma ley se precisan diversas disposiciones para el tratamiento que el sector público debe otorgar a los archivos y que tienden a proteger la utilización de los datos de carácter personal, estableciendo genéricamente lo siguiente: Sólo se crearán, modificarán o eliminarán los archivos, previa disposición del Titular del Ejecutivo, de los Presidentes Municipales y de los titulares de los organismos públicos.

También se regulan los casos en que los datos contenidos en archivos públicos podrán comunicarse exclusivamente a otras instancias de las administraciones públicas estatales y municipales u organismos públicos, cuando se trate, por ejemplo, de la misma competencia o de que se hubiera previsto en la disposición de creación del archivo.

La ley previene los casos en los que las entidades públicas podrán integrar archivos sin el consentimiento de los interesados.

Quiero señalarles a ustedes que el sector privado tiene muchas bases de datos.

Podemos hablar de esas cadenas de tiendas departamentales, de la correspondencia o documentación y de las ventas a distancia y de la prospección comercial de actividades similares.

Al respecto la ley establece que para la creación de archivos que contemplan datos de carácter personal de parte del sector privado, podrán crearse cuando sean necesarios para lograr los objetivos legítimos, pero deben de dar aviso a la Comisión de su creación.

Quiero también informar que genéricamente la ley concede al ciudadano, de manera expresa, varias acciones: Acceso a sus datos personales; rectificación de sus datos; oposición y cancelación de datos.

Concluiré diciendo tres cosas: Solamente el estado de Colima cuenta con la legislación específica para proteger a las personas del uso indebido de sus datos personales.

En algunas otras entidades las leyes contemplan el acceso a la información pública, pero resultan insuficientes para su adecuada regularización.

Dos. La aplicación de la ley en nuestro Estado ha encontrado cierta complejidad, particularmente con motivo de que un alto número de archivos del sector privado que contiene datos personales de habitantes de Colima se concentran desde entidades ajenas, donde no es factible aplicar las disposiciones normativas en observancia, al principio de territorialidad de la ley.

En consecuencia, es deseable que el resto de los estados cuando tengan ya su ley de protección de datos personales, tome en cuenta esto que nosotros le llamaríamos vacío legislativo.

Por último. Cuando se vaya a tutelar la Ley de Protección de Datos Personales es importante contar con recursos humanos, tecnológicos y financieros que hagan posible aplicarla en forma de vida exitosa.

Moderador: María Marván Laborde. Comisionada Presidenta del IFAI.

Agradecemos muchísimo a la Comisionada Presidenta del estado de Colima, creo que apunta una de las cuestiones fundamentales de la Ley de Protección de Datos Personales y el problema de la territorialidad y como lograr realmente armonizar la Federación, el estado y es el municipio y al mismo tiempo controlar las bases de datos que están en Colima o que afectan a la gente de Colima, sin lugar a dudas uno de los problemas centrales que hay que tomar en cuenta en esta legislación.

Sin más prolegómenos porque el tiempo nos corretea, le doy ahora la palabra al Consejero del Instituto Coahuilense de Acceso a la Información Pública, Alfonso Raúl Villarreal, me he permitido presentarlo solamente por la Comisión en la que están, no haciendo caso omiso de sus muy valiosos currículum, sino en razón de que su representación institucional ya está aquí como tal.

Ponente: Alfonso Villarreal Barrera. Consejero del Instituto Coahuilense de Acceso a la Información Pública.

Yo les voy a hablar brevemente acerca de la situación de la protección de los datos personales en el estado de Coahuila.

En octubre de 2003 en el estado de Coahuila se envió al Congreso del estado un paquete de cuatro anteproyectos de ley en relación a la transparencia.

La primera fue de acceso a la información. La siguiente fue de archivos públicos. La siguiente fue la que da creación al Instituto Coahuilense de Acceso a la Información Pública y, finalmente el anteproyecto, la Iniciativa de Ley de la Protección a la Intimidad de las Personas.

Las primeras fueron aprobadas en el Pleno del Congreso y esta última quedó pendiente su aprobación.

Mencionaré muy brevemente cuál es el contenido de ese anteproyecto de ley y cuáles fueron algunas de las reacciones de los grupos sociales en relación a este anteproyecto, a esta Iniciativa, para finalmente concluir en cómo se ha ido subsanando la carencia de esa normatividad y como es urgente la regulación de esta materia.

El contenido de la ley en sus aspectos medulares contemplaba garantizar el derecho a la intimidad de las personas y el derecho de la protección de los datos personales, a partir de los principios de la calidad de los datos, la transparencia o la publicidad del tratamiento, el consentimiento informado, la seguridad de los datos, la interpretación constitucional más favorable, la libre circulación de los datos con fines lícitos. Y consideraba también el garantismo de los datos en poder de las entidades públicas y de los particulares.

En la iniciativa el derecho a la intimidad se consideró como un poder autónomo de las personas, con la posibilidad de que estas personas definieran libremente qué actividades o qué aspectos formaban parte de su círculo intimo, de su círculo personal o su círculo familiar.

Además este anteproyecto determinaba los derechos de ciertos grupos en torno a una relación jurídica con el estado u otros particulares y se pretendía establecer como un interés público y social la protección a la intimidad de ciertos grupos, como eran los niños y las niñas, las mujeres, la juventud, los adultos mayores, las personas con preferencias sexuales diferentes y las personas con capacidades diferentes, a estos grupos se les reconocía como grupos vulnerables y en ese sentido gozarían de una tutela prevalente en la medida que su

derecho a la intimidad resultara restringido o afectado por la discriminación.

Estableció también este anteproyecto las bases para la prohibición de afectar la esencia al derecho a la intimidad, ninguna persona podría ser obligado a declarar sobre ideología, sobre religión, sobre cuestiones de honor, creencias o preferencias o algunos otros datos personales que afectaran sensiblemente su dignidad.

Destacaba también lo relacionado a que los inculpados no podrían ser sometidos a ninguna prueba que pudiera afectar su intimidad y en un caso de hacerlo tendría que existir el consentimiento expreso.

Se consideraba a la comunicación del inculpado y su defensor como algo privado e inviolable y que los centros penitenciarios deberían de tener un lugar para asegurar este derecho.

Ante la violación de los datos personales y la intimidad de las personas toda diligencia o prueba carecería de valor probatorio y además, si se practicaba alguna prueba tendría que ser con carácter confidencial.

De esta manera se establece que la vida privada y la vida familiar son inviolables en los términos de la ley.

Reconoce algunas otras materias, como es la materia de salud, en donde la máxima protección a la intimidad del paciente es obligatoria para el médico el secreto profesional del médico o el secreto profesional de los abogados o cualquier otro profesionista que tuviera acceso a datos personales y con esto estar íntimamente ligado a la privacidad de la persona.

Abordaba también este anteproyecto el secreto del periodismo profesional. Establecía que ninguna autoridad podía obligar a un profesional del periodismo a revelar sus fuentes.

Y en materia religiosa asentaba la obligación de guardar el secreto de la intimidad de los fieles por parte de los confesores o sacerdotes o cualquier otro ministro de culto.

Se establecía la protección de los datos personales como una garantía individual de interés legítimo, que genera información que es irrenunciable, que es intransferible y negociable e indelegable.

Y puntualizaba en lo relacionado al interés legítimo, en donde las personas con este interés tendrían el derecho de conocer, de acceder, rectificar, ratificar o cancelar los datos personales que tuvieran o las entidades públicas o las entidades particulares.

Establecía también este anteproyecto de ley el sistema garantista de la acción con dos herramientas jurídicas que eran la acción para exhibir proteger el dato personal y la otra que era el juicio para la protección del derecho a la intimidad.

Este anteproyecto a los ojos de expertos era un anteproyecto bastante completo, pero para otros no lo era tanto y sí era restrictivo, de tal manera que se generó en la sociedad la percepción que era una ley mordaza y comenzaron a surgir algunas cabezas de periódicos como las siguientes: “Bloquearán en Coahuila la libertad de expresión”, “Perderá la comunidad el derecho a informarse”, “Revisarán 35 diputados la Ley de Datos Personales”, “Critican los expertos lo relacionado con la Ley de Datos Personales”.

Todo esto dio como resultado final que el Congreso del estado dejara pendiente de aprobación esta iniciativa de ley. Por tal razón el marco jurídico que tiene el estado de Coahuila en materia de transparencia y acceso a la información está cojo. Tenemos solamente la Ley de Acceso, la Ley del Instituto, la Ley de Archivos y traemos pendiente esa parte.

Por disposición constitucional el Instituto Coahuilense de Acceso a la Información es el garante de la protección de los datos personales. Sin embargo, carecemos del Marco Jurídico para

poder llevar esto con apego a la ley, y esto lógicamente representa inseguridad jurídica tanto para las entidades públicas y privadas en el manejo de los datos, como para las propias personas que en algún momento se pudieran ver afectados en su vida privada, familiar, su integridad física, genética, moral.

A manera de conclusión yo quisiera exponer que existe una urgente necesidad de regular esta materia de datos personales, y el respecto al derecho a la intimidad de las personas en el estado de Coahuila, y que seguramente el ICAI impulsará una iniciativa de ley en la materia.

Moderador: María Marván Laborde. Comisionada Presidenta del IFAI.

Agradezco de manera muy cumplida la exposición.

Sin lugar a dudas la exposición nos revela las dificultades del equilibrio entre la libertad de expresión, la protección de datos personales y vale la pena apuntar la novedad de la ley de Coahuila, en donde se habla de la legalidad del secreto de confesión. Sin lugar a duda es una innovación propia de la ley, habrá que ver si también aplica a sicólogos y siquiatras, desde luego.

Ponente: María Pérez Cepeda. Comisionada Presidenta de la Comisión Estatal de Información Gubernamental de Querétaro.

Puede ser que yo sí me ajuste al tiempo, porque en Querétaro tampoco hay Ley de Protección de Datos Personales, y solamente hay algunas disposiciones en la Ley de Acceso a la Información en donde se protegen los datos de los particulares, los datos personales de los funcionaros públicos, también en algunos casos, que se encuentren inmersos en un documento público. Pero más allá de esta protección no existe posibilidad de rectificación de los datos de conocer qué bases de datos existen en las entidades gubernamentales y de interés público. De poder solicitar la supresión de los mismos, etcétera.

Básicamente en Querétaro contamos con la Ley Estatal de Acceso a la Información Gubernamental, que establece lo necesario para garantizar el acceso a la información pública, entendida ésa como toda la información con la que cuenta el estado.

Y por otro lado, y con el fin de no afectar los derechos de terceros se establecen excepciones a esta permisa principal, previendo los conceptos de información reservada y de información confidencial.

Pero como les decía, no hay sistemas de datos personales, no se establece cómo deben de tratarse éstos. No se establecen medidas de seguridad, no se establece responsabilidad para los funcionarios públicos que divulguen datos personales, etc.

El artículo Tres de la Ley Estatal de Acceso a la Información Gubernamental define cuáles son los datos confidenciales, la información confidencial y coinciden con muchas otras legislaciones de acceso a la información, estableciendo como información confidencial la relativa a cualquier dato que pueda ser identificable a una persona, entre otras, la relativa al origen étnico, racial, la que se refiere a características, físicas, morales, emocionales, la vida afectiva familiar, el domicilio, número de teléfono, patrimonio, ideología, etc. Cualquier otra análoga que afecte su intimidad. Y allí está la complicación de entrar al campo de la analogía.

También nos remite a las disposiciones, a los derechos de la personalidad que establece el Código Civil, que más adelante voy a tocar.

Establece la Ley de Acceso a la Información una serie de información que se debe de estar publicando de manera obligatoria y en donde se encuentra la posibilidad de que las personas se opongan a la publicación de sus datos personales como, por ejemplo, la información con la que cuentan los órganos jurisdiccionales, administrativos o del trabajo, tienen que estar haciendo ellos, tienen que estar publicando

extractos de las resoluciones, extractos de los hechos que se están discutiendo y las lista de la partes.

Esto vendría a afectar la intimidad o la privacidad de las personas, pero se salvaguarda esta situación con la posibilidad de que las partes puedan oponer a la publicación de sus datos.

Establece también la responsabilidad del funcionario que divulgue la información reservada o confidencial y dice: "De conformidad con las leyes aplicables", pero no hay otra aplicable a la materia, nos tendríamos que remitir a la Ley de Responsabilidad de los Servidores Públicos, que en el caso no dice nada.

Aquí hay una situación importante también, que nos pasa en Querétaro con esta Ley de Acceso de la Información, porque por una parte establece como información confidencial, que desde luego no está sujeta a plazos de vencimiento y que requieren consentimiento para que pueda ser difundida, del titular de los datos, que es la información confidencial.

Sin embargo, en otro artículo, en varios artículos señala como información reservada, que la naturaleza de la información reservada es que sí está sujeta a plazos de vencimiento y se refiere a que será información reservada, por ejemplo, la de carácter personal que se contenga en los padrones o registros estatales de contribuyentes, la información de carácter personal que se contenga en los expedientes de la defensoría de oficio en material penal o de la defensoría del trabajo o similares en materia civil y familiar; nombres de las víctimas de delitos sexuales o de explotación de menores y las partes en las controversias de carácter familiar.

La información personal contenida en las actuaciones de la Comisión Estatal de los Derechos Humanos para la investigación de denuncias por violaciones a derechos fundamentales; la de carácter personal, contenida en los registros o expedientes del personal académico de la Universidad Autónoma de Querétaro y también de los alumnos.

Encontramos aquí este problema, porque o es confidencial o es reservada. La estaría manejando la ley dentro de estos dos aspectos, y siendo que definitivamente sabemos que la información, los datos personales no están sujetos a ningún plazo de vencimiento, ni requieren someterse a un procedimiento de clasificación de reserva, sino que por sí son ya confidenciales.

Igualmente, el Reglamento de la Ley establece algunas disposiciones en las que se observa el principio de consentimiento para la divulgación de los datos personales que básicamente, como les decía, se encuentra inmersa en la información pública.

Y, bueno, ahí la Unidad de Información tiene que encontrar al titular de los datos, notificarle que hay una solicitud en donde hay información personal suya y si está de acuerdo o no con que se divulguen.

En caso de que no conteste nada, bueno, se entiende negado el acceso a los datos personales y el funcionario tendrá que salvaguardar los datos, pues tachando los mismos del documento.

Con este marco jurídico nos hemos encontrado casos y hemos tenido que resolver algunas solicitudes de información, algunos recursos de revisión en la Comisión Estatal de Información Gubernamental, en donde tiene que ver la solicitud con los datos personales de un tercero o que tiene que ver la solicitud con datos personales de los cuales es titular quien lo solicita.

En las dos situaciones, y con esta, como lo decía, con este marco jurídico ambiguo y lleno de lagunas y sin que exista una disposición específica en la materia, nos hemos tenido que enfrentar a resolver algunas controversias, sobre declaraciones patrimoniales, sobre, digamos, que se solicitaban de un tercero, pues hubo que

negar el acceso a la información y, sobre información, por ejemplo, que solicitaba un militante de otro partido y que quería limpiar su honor diciendo que no había pertenecido al partido opositor, pues también le dijeron no te puedo dar esa información, siendo que él en todo caso era el que tenía derecho a saber si había información suya en ese Instituto político.

Ha habido otros casos también interesantes que tiene que ver con fideicomisos en donde los trabajadores entregaban parte de su sueldo y finalmente no tenían acceso a los contratos de adhesión, no tenían acceso a saber en qué condiciones se habían contratado. Por ahí también hubo que resolver en ese sentido.

Básicamente contamos con disposiciones relativas del código civil en donde se definen los derechos de la personalidad y donde se establece que son ilícitos los actos o los hechos que lastimen el afecto de las personas, la creencia o la consideración de sí misma. También aquí tenemos un problema para probar en qué grado se afecta el honor, la intimidad, la estima o la consideración que de sí mismo tiene uno. Que tal si tiene su estima muy alta.

Se menoscaba el honor, la reputación, el prestigio o la estima que de ellos tengan los demás, se afecte la vida privada o la intimidad de los secretos de las personas. También aquí hay un elemento difícil de probar, en qué grado se afecta o no se afecta la estima de las personas.

También una disposición importante que establece el Código Civil, es en cuanto a la reproducción de la imagen de las personas que también en este sentido habría que contemplar, se tendría que contemplar en la legislación la protección a la propia imagen.

En Querétaro contamos, como les decía, con esta disposición que establece que la reproducción de la imagen de la persona sin su consentimiento y sin un fin lícito es violatoria de los derechos de la personalidad. Básicamente ese es todo el marco jurídico.

Existen algunas disposiciones por ahí en el Código Urbano, en la Ley de Catastro, en la Ley de Educación en donde se puede rectificar algunos datos como el domicilio fiscal de la persona o el domicilio del contribuyente, los datos de los nombres de los menores en la Unidad de Servicios de Educación Básica, las Actas de Registro Civil. Pero básicamente no hay más al respecto que nos pueda apoyar en este sentido y, bueno, yo al igual que mis compañeros comisionados y todo lo que se ha comentado aquí en este foro, pues desde luego reconozco la importancia que reviste el que contemos con una Ley de Protección de Datos Personales. Y, eso es la conclusión final de todo esto.

Moderador: María Marván Laborde. Comisionada Presidenta del IFAI.

Quedan claras las dificultades prácticas que tienen malas definiciones jurídicas iniciales, así como la dispersión de normas de la que me permitiré, al final de esta mesa, hacer unos breves comentarios con relación a Jalisco.

Ponente: Carlos Paniagua Bocanegra, Consejero del Instituto de Transparencia y Acceso a la Información Pública del Estado de México.

La protección de datos personales en el Estado de México. Tenemos una gran ventaja, a diferencia del nivel federal, nuestra Constitución en su artículo 5, párrafo segundo y tercero establece claramente, expresamente que el Estado garantizará el derecho a la información, que el Estado garantizará la protección de los datos personales, que el Estado garantizará la transparencia de la función pública.

Y es importante porque es algo que no han considerado los servidores públicos que niegan o no proporcionan completa la información solicitada. El incumplir con un mandato constitucional provoca una grave responsabilidad, que inclusive en el caso de los consejeros es motivo para que se nos suprima del cargo.

Esta modificación de la Constitución estatal es del 30 de abril del 2004, entró en vigor el uno de agosto de 2004 y dio origen a la Ley de Transparencia y Acceso a la Información Pública del Estado de México.

También es muy clara esta ley, el artículo Primero establece que esta ley es reglamentaria de los párrafos segundo y tercero del artículo Quinto Constitucional, garantiza el derecho de acceso a la información y protege los datos personales.

¿Qué son datos personales? Caemos en el error, nuestro legislador, de copiar en este sentido las leyes extranjeras, en caso particular la Ley 25.326 Argentina, identificada como Ley de Protección de Datos Personales Hábeas data, se hace la traducción literal Hábeas data a datos personales, para mí, para mí debería para ser más congruente como información privada.

En el artículo Dos, fracción II, de la Ley del Estado de México se establece como dato personal la información concerniente a una persona física identificada o identificable, como lo pone también la Ley Federal. Pero se ha malinterpretado esto, porque se ha malinterpretado, y no por parte del Instituto, de que el nombre es un dato personal y que se tiene que proteger, es un absurdo. El nombre conforme al principio que marca nuestro Código Civil del Estado de México es el elemento que individualiza a la persona, cómo se va a identificar a la persona si no es por su nombre, cómo no se va a precisar la información que debe ser protegida si no es con el nombre de la persona.

Por otra parte, dice que es información pública la relativa, la referente, entre otras, al domicilio y al número telefónico.

Hemos visto aquí desde la Ley Española, Ley Orgánica de Protección de Datos Personales, que la doctora María Antón nos presentó, cómo la Constitución Española, cómo la legislación alemana, la francesa, limita, establece que la información, la protección de datos personales se lleva a cabo con los límites de la garantía de la intimidad, de la privacidad, del honor, como lo dice la Ley Argentina, se debe proteger el honor, el derecho del honor y el derecho a la intimidad.

Cuando a mí me piden la copia de un documento público, una solicitud de un establecimiento comercial, no la voy a dar porque tiene el nombre, porque tiene el domicilio, quien está en contra de esta idea, que respeto mucho, pero que creo que no tiene un sentido jurídico, porque dice: es que el domicilio está protegido por el artículo 16 Constitucional, efectivamente; pero el domicilio que marca el artículo 16 Constitucional se refiere a la inviolabilidad de domicilio, nadie puede ser molestado dentro de su casa, nadie puede ser aprendido dentro de su casa, no puede ser el cateo dentro de su casa, esos son los actos de molestia que la Suprema Corte de Justicia de la Nación ha aceptado en la jurisprudencia referente.

Si analizamos en una interpretación sistemática, armónica, gramatical, el concepto que marca el artículo 2, fracción II, sobre dato personal, también nos tenemos que referir al 25, fracción I y al 55, fracción I, de la Ley estatal, que dice: El dato personal es una información confidencial. No puede divulgarse si afecta a la privacidad de las personas.

El citar en un documento el domicilio, el número telefónico ¿afecta el honor de las personas, afecta la privacidad, afecta la intimidad de las personas? Yo creo que eso es parte de la modificación que debemos de proponer al Legislativo que se modifique.

Debemos tener una ley con técnica jurídica, con técnica legislativa, una ley que todo mundo entienda. Tenemos la ventaja de que es una ley válida, conforme al principio de Kelsen, surge de la norma fundamental.

Hay que hacerla eficaz ¿cómo? Con técnica jurídica y técnica legislativa para evitar confusiones.

Esta ley crea el Instituto de Transparencia de Acceso a la Información Pública, como organismo público descentralizado, no sectorizado en reforma publicada en diciembre de 2004.

Los servidores públicos tenemos la obligación de emitir resoluciones respecto a las solicitudes de los particulares en forma debidamente fundada y motivada, cumpliendo el artículo 14 y 16 constitucional. Si es así cómo vamos a fundamentar una o vamos a entregar parchada como una figura que se habla, de una versión pública que no tiene ningún sustento jurídico, el tachar en este documento el nombre y el domicilio.

¿Qué acaso nuestras leyes no establecen claramente que un documento no puede ser público, no puede ser tachado ni enmendado, y que en dado caso una simple línea delgada puede subsanarse el error? Lo estamos violando, y por eso es que en lo personal yo quiero convocar a un congreso mexiquense de derecho a la información, para efecto de considerar y establecer, hacer más claro y más válido, más eficaz este derecho a la información.

Ponente: Vicente Hernández Delgado. Comisionado Estatal para el Acceso a la Información Pública del Estado de Sinaloa

Precisamente en abono del tiempo no voy a leer una gran parte de la ponencia. He tratado de resumir una primera parte de mi intervención en tres etapas, que desde mi punto de vista ilustran el tratamiento de la cuestión.

Una primera etapa tiene que ver con la tutela jurídica por parte de la legislación de primer nivel y la legislación secundaria del derecho a la intimidad y a la privacidad de las personas.

Como ya se ha dicho esta parte reguladora en la Constitución General de la República, y particularmente en el artículo 16 se refiere a la protección, a estas partes que corresponden a la esfera de la intimidad y la privacidad, como es la protección a la inviolabilidad domiciliaria, y a la inviolabilidad de las correspondencias secretas o privadas de las personas.

Y en la legislación secundaria, en este mismo nivel de protección jurídica, de tutela jurídica a la privacidad de la intimidad, encontramos una referencia muy tenue, muy inconsistente al derecho, a la protección, al derecho de las personas a la propia imagen, cuando se establece la figura del llamado daño moral en la Legislación Penal y en la Legislación Civil, tanto a nivel federal como a nivel estatal.

Y en lo que se refiere a la otra figura jurídica que también se tutela y que forma parte de este derecho a la intimidad, a la privacidad que hemos estado señalando, está el derecho al honor, que también está regulado en la legislación penal federal y en la legislación penal de los estados y en cierta legislación de carácter civil.

Este derecho al honor incluso va acompañado de una acción punitiva del Estado, al imponer o al establecer las figuras de la difamación y de la calumnia, como figuras equivalentes precisamente a la reparación del derecho al honor o, más bien, la protección del derecho al honor de las personas.

Aparte de esta legislación, que todos ya conocemos en las escuelas de Derecho, está una segunda etapa, que es la que me parece que empieza a definir, de manera incipiente, la regulación de los datos personales en nuestro país.

Esta etapa tiene que ver con el auge de las tecnologías de la información y las comunicaciones, y que se expresa fundamentalmente en la imposición de figuras o de tratamiento de figuras, de conductas que en términos académicos el derecho informático va a retomar.

Por ejemplo, me refiero fundamentalmente a reformas legislativas al Código Penal Federal, al

Código Penal del Distrito Federal y al Código Penal de Sinaloa, en donde de manera más o menos diferenciada se va a regular a los delitos electrónicos y a los delitos informáticos, como figuras que lesionan de alguna manera, entre otras actividades, entre otras conductas lesivas, precisamente a la intimidad y la privacidad de las personas.

Y de manera consecuente la reforma de 2000 ó 2002, de mayo de 2000 ó 2002, no recuerdo exactamente el año, al Código de Comercio, al Código Civil, al Código de Procedimientos Civiles y a la Ley Federal de Protección al Consumidor, para regular las actividades en términos de comercio y contratos electrónicos, en donde se establece la figura del mensaje de datos, es una figura que va ser objeto de protección y de definición, precisamente en la legislación civil y mercantil, y que tiene como finalidad el de fijar, diseñar precisamente esa forma de comunicarse o de establecer informaciones de carácter mercantil, a través precisamente de medios electrónicos, ópticos, visuales o de cualquier otra tecnología, como se considera al mensaje de dato usual, cualquier tipo de información o de comunicación que se dé a través de ese tipo de instrumentos, como mecanismos precisamente para formalizar acto de comercio.

También existe mención a esto en la Ley Federal de Derechos de Autor, en un apartado que se refiere a la protección de datos personales y de programas de cómputo. Precisamente el término, la protección de bases de datos, está asociado fundamentalmente al auge en las tecnologías de la información y de las comunicaciones, y asociado indiscutiblemente, precisamente a la protección de los datos personales.

También tenemos estos elementos en la legislación financiera, sobre todo aquella ley que regula a las sociedades de información crediticia, sobre todo lo que se ha dicho mucho sobre las actividades del Buró de Crédito y otras; la Ley de Geografía, Estadística e Informática, para no extenderme demasiado.

Una tercera etapa que yo considero y que tiene que ver precisamente con el tema que estamos tratando es la que se refiere a la aparición de la legislación federal de acceso a la información pública y a la legislación estatal de acceso a la información pública en la mayoría de los estados, en donde se introduce en la mayoría de las legislaciones la figura del *Hábeas data*, como garantía procesal que tiende precisamente a proteger los datos personales. Pero establecer un mecanismo que permita que el ciudadano, que el titular de los datos pueda precisamente proteger sus datos.

Y aquí encontramos una dificultad. En el caso de Sinaloa existe precisamente mención a la figura de la *Hábeas data*, como existe en muchas otras legislaciones de acceso a la información pública, pero es una legislación que deja más dudas e interrogantes.

Para empezar, el capítulo referente a la información reservada y confidencial es mucho más explícito en materia de información reservada que de información confidencial y como se deja precisamente la regulación de este tema a la información confidencial a la figura de la *Hábeas data*, no se aclara suficientemente pero ahí está.

Si embargo, como la figura de la *Hábeas data* es una garantía procesal, tampoco se establece adecuadamente el procedimiento, se señala ciertamente que la Comisión de Acceso a la Información Pública de Sinaloa es la que va precisamente a conocer y a resolver este tipo de conflictos que se generen entre el titular y las personas, ya sean responsables del registros o ficheros que hayan hecho uso ilícito sin autorización de los datos personales o las intromisiones de terceros a esa esfera personalísima de los individuos.

En Sinaloa existe una legislación que duerme el sueño de los justos, hay un proyecto de ley de protección de datos personales que se presentó al Congreso en junio de 2003, obviamente la aspiración sería que ese proyecto se sacara del

archivo y fuese discutido, valorado y con las actualizaciones que fuesen pertinentes, pues proveer a esa etapa necesaria que se advierte en el país y que tiene que ver precisamente con el establecimiento de la Ley de Datos Personales.

Como la figura de la *Hábeas data* es una figura regular en casi todas las legislaciones de acceso a la información, es más clara todavía en la legislación federal de acceso a la información porque ahí hay un capítulo referente a la protección de datos personales y además existe un Reglamento que regula el tema.

Me permito nada más leer dos cuartillas que fija la posición nuestra con respecto a este asunto del procedimiento que hubiera de regularse.

"La protección de los datos personales en la actualidad amerita un mecanismo de protección jurídica efectivo, ya que el derecho a la privacidad e intimidad sustentados en los pilares que edifique el derecho fundamental de la *Hábeas data*, debe tener como finalidad inicial el que cualquier persona pueda acceder a la información que sobre ella existen en cualquier registro o banco de datos".

"Para ello es preciso ejercitar un procedimiento especial, relativo a la solicitud de información de datos personales, con plazos y términos bien definidos, en donde se hace preciso inicialmente estructurar esta solicitud en la entidad pública en donde se encuentren este tipo de información personal".

Debo decir que en la doctrina argentina, en la legislación argentina el trámite, el procedimiento para hacer efectiva la protección de datos personales es ante un tribunal de lo civil.

En la legislación de los estados y en la legislación federal se otorga esa potestad, esa responsabilidad a las Comisiones de Acceso a la Información.

Esta dependencia deberá "reseccionar" esta solicitud integrando un procedimiento administrativo en torno al mismo, con el propósito fundamental de compartir con el solicitante los archivos que requiere. Lo anterior se fundamenta en el derecho que tiene todo titular de los datos a conocer el tipo y calidad de información que poseen y procesen en cada una de las dependencias públicas. El único requisito de fondo que debe contemplar esta solicitud es la identificación plena del solicitante.

Un segundo momento procesal que habrá de contemplarse en se procedimiento se deriva de la posibilidad jurídica que tiene cualquier persona, titular de los datos personales de accionar en torno a la actualización, rectificación, supresión o modificación de los datos que consten en las entidades públicas, relativos a su individualidad, para lo cual el detonante ante las dependencias sería la manifestación expresa de la voluntad del sujeto, tendiente a realizar la trasformación de la información y los elementos probatorios que la persona pueda aportar para comprobar de la forma más clara posible la base jurídica que sustenta su afirmación.

Ambos momentos procesales deberán tener términos breves y precisos y que contribuyan a garantizar la protección integral de este derecho fundamental. Aunado a esto se requiere la vigilancia y tutela de un órgano especializado en los procesos de información que se constituya como la garantía procesal que proteja la identidad, la privacidad, la intimidad y la autodeterminación informativa que cada persona debe ejercitar.

El titular de los datos podrá exigir en todo momento y sin plazos perentorios que los sujetos obligados que administren, manejen, archiven, posean y conserven en su poder información confidencial en base de datos, archivos o registros garantice un adecuado uso y tratamiento de los datos personales.

Moderador: María Marván Laborde. Comisionada Presidenta del IFAI.

Agradezco muchísimo, no quisiera concluir este panel, sin hacer un comentario que nos ha llamado muchísimo la atención, en el Código Civil del Estado de Jalisco se aprobaron una serie de reformas que en realidad fue insertar prácticamente como Caballo de Troya dentro del Código Civil una Ley del Protección de Datos Personales que consta de 39 artículos, en los cuales se tratan diferentes materias, inclusive, el manejo de la información crediticia, creo que es importante porque releva esto la complejidad jurídica que existe en el país en el tema.

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

Mesa 9

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

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

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

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

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

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

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

Tales documentos son los siguientes:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Conferencia Magistral de Clausura
Firma de Cartas de Intención

Conferencia Magistral: Sergio López Ayllón.

Doctor en Derecho, profesor e investigador de la División de Administración Pública del CIDE. Investigador del Sistema Nacional de Investigadores y sus principales líneas de investigación atañen al acceso a la información, al derecho de la información, a las políticas de regulación, a la reforma de la administración pública, a la sociología del derecho y transparencia.

Quiero, en primer lugar, agradecer, como es de rigor, a los importantes organizadores de este Encuentro su muy gentil invitación, para dictar esta Conferencia de Clausura.

Agradecimiento que, debo decir, muy matizado, pues rápidamente se transforma en agobio y si no en angustia por tener que exponer ahora frente a todos ustedes, que durante tres días han discutido ya con conocimiento, rigor y profundidad, las diferentes dimensiones y problemas que implica la protección de datos personales en nuestra globalizada sociedad de la información.

Resulta difícil, cuando no pretencioso, tratar de añadir algo nuevo a lo ya debatido; de los problemas ciertos que plantean las tecnologías de la información para la vida privada, hasta la construcción aún incierta de un derecho fundamental a la protección de datos personales, cuyos contornos exactos parecen aún difusos.

De los problemas normativos que plantea la regulación de los datos personales para los gobiernos y las empresas, hasta aquéllos más técnicos, relacionados con la seguridad de los sistemas de datos personales.

Un tema insoslayable para este país, que con mucho gusto los recibe y que ha consumido gran parte de este encuentro, es el relativo a la necesidad y contenido posible de una Ley de Protección de Datos para este país.

Hemos tenido la fortuna de contar con la presencia de algunos de los más importantes expertos iberoamericanos en esta materia, y créanme que sus contribuciones han sido muy importantes y enriquecedoras para informar el debate necesario acerca de esta ley.

Mi intervención se va limitar a subrayar algunas ideas centrales que me parece se desprenden de las intervenciones durante estos días y atreverme a profundizar en algunos de los aspectos que me parece deberían ser objeto de una reflexión cuidadosa, por parte de nuestros legisladores, que a

veces, entusiasmados con una buena idea, se lanzan con brío a establecer un marco regulatorio, cuya operación completa no parece preocuparles demasiado.

Quizás en esto estamos solamente repitiendo esa idea tan arraigada en nuestra cultura y en mucho compartida con otros países de Iberoamérica, que los problemas se pueden resolver a golpe de ley y que ésta actuaría como una especie de sortilegio, de barita mágica, cuya mera invocación parecería ser suficiente para transformar una realidad compleja.

Se olvida con frecuencia que una ley es sólo el vehículo de una política pública que supone objetivos claros y mesurables, recursos, instituciones y voluntad política.

Me parece que existe un consenso claro.

El mundo ha vivido, en los últimos 150 años, una vertiginosa revolución de las tecnologías de la información y la comunicación, que han cambiado profundamente, no solamente los mecanismos de intercambio, sino el conjunto de las relaciones humanas.

Hago un muy breve recuento.

Hacía 1840 Sir Charles Winston y Samuel Morse inventan el telégrafo.

El grámofo aparece a principios de la segunda mitad del siglo XIX.

En 1876 Bell envía el primer mensaje telefónico.

Para 1895 Marconni transmite mensajes inalámbricos.

Hacia 1894 son proyectadas las primeras películas.

Ya en el siglo XX, en 1904 se transmiten imágenes por aparatos telegráficos.

En 1906 se transmite la voz humana por radio y en 1920 se lograr enviar las primeras imágenes de televisión.

Las primeras redes de radio se establecen hacia 1929 y las de televisión en los treintas.

Las primeras computadoras aparecen en los años cuarenta, y el Pájaro Madrugador, primer satélite comercial de intercomunicación, es lanzado hacia 1962.

Hacia principios de la década de los sesentas, la alianza entre las telecomunicaciones y la informática permite el vertiginoso desarrollo del Internet, la red de redes, que para los noventas alcanza una cobertura mundial pocas veces imaginada.

Las innovaciones tecnológicas que han ocurrido en la última década, en particular la convergencia a las telecomunicaciones, la informática y los medios audiovisuales, a través de la tecnología digital, están produciendo una profunda revolución en la capacidad social de procesar, almacenar y transmitir información.

Los servicios relacionados con la información han creado auténticos espacios virtuales, deslocalizados y no jerarquizados donde circulan millones de unidades de información y amplían, sin duda el horizonte de la acción humana.

Diversos autores han analizados estos fenómenos desde muy diversos ángulos. Me importa destacar aquí como por ejemplo para Manuel Castells una conclusión fundamental es que existe una tendencia histórica clara en la que los procesos y funciones dominantes en la era de la información están cada vez más organizados alrededor de redes. Las redes constituirían la nueva morfología de nuestras sociedades y la difusión de la lógica de las redes modifica también sustancialmente la operación y producción de los procesos sociales de producción, experiencia, poder, cultura e incluso identidad.

Algunas de las implicaciones de lo anterior son fundamentales para comprender cómo estos cambios están modificando también las concepciones tradicionales de lo público y lo privado, pues introducen una lógica diferente que conduce a que las fronteras de estos conceptos, de por sí siempre difusas, se vuelvan aún menos claras y útiles para el análisis.

No es excesivo decir que la tecnología de la información ha trastocado las fronteras entre lo público y lo privado. Los flujos de información y la capacidad tecnológica y social de producir, almacenar y transmitir información en espacios virtuales deslocalizados y que por ello escapan a los mecanismos tradicionales del control estatal, suponen una transformación radical de alguna de nuestras categorías de análisis de las cuales cuya utilización no siempre alcanzan dar cuenta cabal de los mecanismos que estamos observando.

Por todo ello, me parece que el problema de la regulación de datos personales tiene una complejidad doble. Por un lado, intenta regular un campo movedizo como lo es el de los datos personales, cuyas fronteras son difusas y que además está en constante movimiento derivado de su intima vinculación con el desarrollo de las tecnologías de la información.

Por otro lado, pretende establecer mecanismos de regulación sobre flujos de información que transitan por sistemas de localizados o fácilmente deslocalizables y que por ello escapan a los mecanismos tradicionales de control estatal.

Quiero precisar que no quiero implicar que esas dificultades deben inhibir la actividad regulatoria del Estado. Todo lo contrario, lo que quiere decir simplemente es que expliquen parte de la dificultad del asunto y le añaden dimensiones de complejidad que se deben tener en cuenta y que por lo tanto si queremos construir una legislación que funcione, no puede tratarse como si enfrentáramos un problema regulatorio tradicional y requerimos de una enorme claridad en los objetivos que estamos tratando de conseguir con una intervención en este campo.

Baste simplemente añadir, como ya se ha hecho patente aquí, que la dimensión transnacional del fenómeno obliga a una coordinación de los reguladores, a fin de lograr siquiera alguna eficacia en este campo.

Ya se ha hablado en este foro ampliamente sobre los llamados modelos de regulación que simplificando se llaman el europeo y el americano y no voy a insistir en ello. Creo que también se ha enfatizado suficientemente que existe un acuerdo básico sobre los principios que deben regir la protección de datos personales, con sentimiento, calidad, pertinencia, confidencialidad, seguridad.

Quisiera completar simplemente con algunas cuestiones que me preocupan respecto de la propuesta de ley que actualmente se discute en el Congreso mexicano, pero que ilustran bien las dificultades que enfrenta el legislador cuando se enfrenta a estas cuestiones.

Insisto, creo en la necesidad de una legislación, lo que tenemos actualmente, por lo menos en este país es malo por parcial, provisional, fragmentado, que genera asimetrías importantes. Basta pensar por ejemplo en el debate que tenemos alrededor del expediente médico donde ya creamos una asimetría muy importante entre la regulación al sector público y al sector privado en esta materia.

Quizás también esto explica por qué nuestra Ley de Acceso a la Información contiene un capítulo que cuando se diseñó se quería provisional en materia de protección de datos, porque teníamos un vacío completo en la materia y no podíamos avanzar en la materia de acceso sin establecer al menos los principios básicos en materia de protección de datos en materia gubernamental.

Sin embargo, obviamente la materia es mucho más amplia, tiene mucho mayor complejidad, pero tampoco se puede borrar la experiencia ya adquirida en estos años en esta materia y

algunas de las lecciones que de ella hemos sacado.

Finalmente, también creo y estoy convencido que una legislación mala produce efectos perversos, aun en ocasiones más graves de los que pretende corregir, o simplemente se vuelve inoperante o en subterfugio para que en sus lagunas sirva de fermento a la simulación o peor a la corrupción.

En este sentido, me gustaría repasar tres o cuatro ideas muy brevemente con ustedes.

Una primera tiene que ver con cuál es el objeto de una legislación en materia de protección de datos personales. ¿Se trata de proteger un derecho fundamental? ¿Es éste la vida privada? ¿O se trata de un nuevo derecho como se ha insinuado aquí: un derecho a la protección de datos personales? si este es el caso, ¿cuáles son los contornos de este derecho fundamental, a quién obliga y cómo lo obliga?

O más bien se trata de regular los mercados de información y si este fuera el caso, ¿cuál es el objeto de la intervención regulatoria en este aspecto? ¿Qué pretendemos con regular estos mercados y, sobre todo, cómo se justifica la intervención del Estado en esta materia?

Me parece que estos son dos problemas distintos que suponen mecanismos y objetivos de regulación distintos. Si, por ejemplo, se trata de la protección de un derecho fundamental y admitimos que el principio básico es el de la autodeterminación informativa, bastaría, quizás, simplemente establecer las instituciones y procedimientos que aseguraran que las personas pueden ejercerlo.

Quizás, en el extremo, la intervención gubernamental se enfocaría a reducir las asimetrías de información y generar las condiciones que propiciaran que los ciudadanos pudieran ejercer este derecho a la autodeterminación informativa.

En cambio, si se trata de la regulación de los mercados de información y de sus instituciones, por ejemplo, la sociedad de información, entonces me parece que el problema regulatorio es distinto y supone una serie de decisiones de política pública muchas más complejas y un diseño institucional distinto.

Si además, éste fuera el caso habría que justificar la acción del gobierno e incluso determinar si la regulación es la mejor manera de intervenir o si no existen otras alternativas más viables dadas las condiciones de un mercado determinado.

El ejemplo básico sería la autorregulación, pero habría otros mecanismos a los cuales se podría recurrir.

Alguien podría argumentar con razón que estas dos cuestiones se implican mutuamente, yo convengo en ello, pero me parece que al menos diferenciar una de otro, ayuda en mucho a generar un diseño legislativo con mayor viabilidad y mucho me temo que la propuesta de ley que hoy discute el Congreso mexicano estas dos cuestiones están francamente confundidas.

Déjenme ilustrar un solo ejemplo de esto, cualquier legislación debe estar soportada por una base jurídica constitucional suficiente.

Y yo me preguntaría: ¿Cuál es la base jurídica constitucional sobre la cual el Congreso mexicano puede emitir o expedir una legislación en esta materia? Y aquí encuentro que francamente este sustento es débil, es débil respecto de la protección de datos personales, aunque quizá ahí podríamos argumentarlo, pero es mucho más débil respecto de las sociedades de información.

¿Cuáles son, entonces, las facultades expresas del Congreso mexicano para legislar en esta materia? La cuestión no es banal, porque si el sustento constitucional no es sólido, entonces la acción regulatoria puede estar destinada al fracaso.

Esta cuestión que parece tan obvia, me permito comentarlo, ni siquiera está discutido en el proyecto de dictamen de esta ley en el Congreso y me parece que es ya significativa.

Pero lleva a otros problemas respecto al nivel de gobierno apropiado en esta materia.

¿En el caso concreto de México es una legislación de carácter federal o estatal? En el proyecto que tenemos enfrente es una mezcla curiosa, porque por un lado aparenta ser una legislación de carácter federal, al menos respecto de los órganos o las entidades públicas federales, pero parece dejar completamente de lado los órganos y entidades de gobierno de carácter estatal o municipal y tendríamos que convenir que estas organizaciones también manejan datos de carácter personal.

En cambio, respecto de las sociedades de información y de las organizaciones como se refiere el proyecto, admite casi implícitamente una regulación de carácter federal, e insisto en la pregunta fundamental: ¿Cuál es el sustento constitucional para esto?

Quizás mi reflexión me llevaría a que probablemente habría que considerar la conveniencia, incluso, de plantear una reforma constitucional, para que esta materia quedara bien definida desde su origen.

Pero los problemas jurídicos constitucionales no son los únicos. Creo que hay otras cuestiones que me preocupan respecto del diseño institucional incluso de cuestiones de carácter procedimental.

Brevemente me refiero a las cuestiones institucionales. Ya se ha hablado aquí de los diferentes modelos, y se insiste mucho en la autonomía de los órganos.

Sin embargo la pregunta relevante es autonomía para qué o de qué. Y aquí, insisto, me parece importante diferenciar las funciones de protección de datos personales que puede tener una agencia administrativa, y que simplemente interviene en un nivel intermedio respecto de la intervención el Poder Judicial, si admitimos que, en principio, en nuestros sistemas la garantía última de los derechos fundamentales se encuentra en los poderes judiciales, cuestión que obviamente alguien podría argumenta que no, pero parecería que ésta es la tendencia.

O bien, si se trata de una autoridad reguladora de un mercado de información, que le da un carácter distinto, y que incluso me llevaría a cuestionar la necesidad de un órgano de carácter colegiado.

Si se trata de una autoridad reguladora, la autonomía administrativa se justifica por razones técnicas, como existe en otro tipo de industrias de redes, y entonces nos lleva a un diseño institucional definido. Distinto probablemente de una agencia cuya función central fuera la protección de datos personales a partir de una óptica de protección de derechos fundamentales.

Quizá estos modelos son combinables. Insisto, lo que resulta fundamental es entender cuál es la naturaleza de la intervención del órgano administrativo en esta materia, puesto que estamos admitiendo que no es un órgano de carácter jurisdiccional en sentido estricto.

Hay otras cuestiones preocupantes, por ejemplo, esta falta de claridad lleva a que se proponga un procedimiento en donde el ciudadano puede recurrir la corrección de sus datos personales directamente ante la entidad privada, ante el órgano administrativo o ante el órgano jurisdiccional, aunque la ley dice que no de manera simultánea no establece prelación ante ellos, y esto evidentemente provocaría problemas procedimentales muy serios que podrían, incluso, a que la eficacia de este mecanismo no fuera el deseable.

Y finalmente cuestiones también de carácter procedimental, que yo me pregunto si hubo consulta suficiente, por ejemplo, con el Poder Judicial. El plazo que establecen para la

intervención de los juzgados de distrito, dada la experiencia que tenemos en las cargas de trabajo que tienen estos tribunales, me hace pensar que los plazos que se están presentando no son ni remotamente viables en las condiciones actuales de operación del Poder Judicial, y no voy a hablar ya de la capacitación que requerirían los jueces para el ejercicio de este derecho.

Creo que habría otras cuestiones en las que ya no quiero abundar por ser demasiado nacionales. Pero sí me parece finalmente que el diseño de una legislación plantea dilemas importantes, y yo me atrevería a pensar que uno de los enormes beneficios de este tipo de encuentros es el intercambio de perspectivas, de experiencias, de diseños, de conocimiento y que permitirán, espero, en el corto plazo que los países de nuestra región cuenten con una legislación adecuada, flexible, dinámica, para este problema que está, sin duda, al centro de las preocupaciones de las sociedades contemporáneas.

Firma de las Cartas de Intención

María Marván Laborde; José Luis Piñar Mañas y Juan Antonio Travieso, titulares, respectivamente de los organismos denominados Instituto Federal de Acceso a la Información Pública, Agencia Española de Protección de Datos y Dirección Nacional de Protección de Datos de Argentina.

Estas Cartas de Intención serán firmadas, por una parte, entre el Instituto Federal de Acceso a la Información Pública de México y la Agencia Española de Protección de Datos.

Y, por la otra, entre el Instituto Federal de Transparencia y Acceso a la Información Pública y la Dirección Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos de la República de la Argentina.

A partir de las competencias y funciones que competen a las partes en cada una de las Cartas de Intención, en relación con la protección de los datos personales, así como del mutuo beneficio que puede resultar del intercambio de sus experiencias y capacidades, en busca de la mayor eficacia y eficiencia en la labor encomendada a las mismas.

Dichas partes manifiestan, a través de estas Cartas, su intención de crear un grupo de trabajo a efecto de que desarrolle un proyecto de convenio de colaboración en materia de protección de datos personales y después de las consultas necesarias formalizar dicho convenio, antes de que concluya el primer semestre de 2006.

Por tanto, en este momento la doctora María Marván Laborde, en representación del Instituto Federal de Acceso a la Información Pública, y los señores José Luis Piñar Mañas, en representación de la Agencia Española de Protección de Datos y Juan Antonio Travieso, de la Dirección Nacional de Protección de Datos personales de la República de la Argentina, procederán a la suscripción de las Cartas de Intención.

María Marván Laborde: Pues a pesar de la sencillez de la ceremonia, muchísimas gracias y enhorabuena, por supuesto a España, por supuesto a Argentina muchas gracias por esto.

José Luis Piñar Mañas: Muchísimas gracias querida María por haber firmado esta *Carta de Intenciones*. Estoy seguro que de este documento surgirán frutos muy importantes, no sólo porque están estampadas nuestras firmas sobre el documento en sí, si no porque hay una magnífica y estrecha relación personal entre los equipos del IFAI y de la Agencia Española de Protección de Datos y esto es lo que en definitiva impulsa los documentos que en algún momento puedan suscribirse.

Estoy ya deseando que se pueda firmar ese convenio formal de colaboración y, sin duda este es el comienzo, como en *Casa Blanca*, de una buena amistad y de lazos más estrechos de cooperación, de colaboración y de una apuesta aún más profunda, si cabe, en aras del derecho

fundamental de la protección de datos y del derecho a la transparencia y al acceso a la información pública.

Juan Antonio Travieso: Quiero agregar fundamentalmente que suscribo todas y cada una de las expresiones del José Luis Piñar Mañas, pero además quiero agregar un punto más, que es la hermandad que nos vincula especialmente en lo que a mí me respecta con respeto a mi país la Argentina con México. Por lo tanto entonces me siento hermanado y me siento orgulloso de poder participar en esto y aumentar, por un lado, mi mexicanidad. Y por otro lado también compartir con María lo que ella también considera su argentinidad.

De manera entonces que unimos esos dos en un proyecto grande y sobre todo, cimentado sobre la Red Iberoamericana de Protección de Datos Personales

Declaración de México

Presídium:

María Marván Laborde, Comisionada Presidenta del IFAI; José Luis Piñar Mañas, Director de la Agencia Española de Protección de Datos Personales y Presidente de la Red Iberoamericana de Datos Personales; Horacio Aguilar Álvarez de Alba, Comisionado del Instituto Federal de Acceso a la Información Pública; Ricardo Sodi Cuellar, Director de la Facultad de Derecho de la Facultad Anáhuac del Norte; Rolando Barrera Zapata, Consejero Presidente del Instituto de Transparencia; Juan Rodolfo Sánchez Gómez, Presidente de la Mesa Directiva de la L Legislatura del Estado de México.

Ricardo Sodi.

La categoría de los conferencistas y de los participantes ha permitido intercambiar experiencias de diferentes países y enriquecer la visión mexicana del derecho a la información y la necesaria reserva de datos que pueden afectar la esfera jurídica, personal y familiar de la población.

En la Facultad de Derecho de la Universidad Anáhuac, consideramos que el derecho a la información, el derecho informático y la protección de datos personales constituyen temas jurídicos que han cobrado autonomía por lo que hemos incluido en nuestro programa de estudios de licenciatura las cátedras de Derecho Informático y Derecho a la Información.

Asimismo, el Programa de Doctorado en Derecho que se imparte en convenio con la Universidad Complutense de Madrid, incluye la cátedra de Derecho Informático, donde se tratan aspectos de legislación comparada entre México y la Unión Europea, relacionada con el acceso a la información pública y la protección de datos personales.

El inexorable avance de la tecnología ha rebasado con mucho la regulación civil, penal y administrativa relacionada con el intercambio de datos personales.

En este foro hemos podido conocer los avances y experiencias de otros países hermanos en esta materia y a efecto de aprovecharlos para impulsar una legislación mexicana al respecto, nos pronunciamos por una regulación adecuada de la protección de datos personales, donde se preserve la dignidad de la persona y los altos valores de la privacidad y permisibilidad con que se maneje la información.

Se deberán incorporar figuras como la autorización del titular de los datos personales, a efecto de poder disponer de ellos y la correlativa prohibición de usarlos con las sanciones penales y la determinación de la responsabilidad civil en caso de incumplimiento.

La información debe ser manejada con un contenido eminentemente ético, respetuoso de las garantías individuales, reservado, toda vez que afectar la esfera de intimidad de las personas puede dar lugar a la afectación de la honra, fama pública o consideración que la sociedad tenga de determinada persona.

Consideramos que no sólo se trata de una simple reforma que pueda ser incorporara a un Código Civil o a un Código Penal, se trata de todo un cambio en la percepción jurídica de estos aspectos tanto a nivel federal, como local.

Deberán ser leyes especializadas sobre la materia que, inclusive, tipifiquen delitos en caso de transgresión y establezcan los parámetros para determinar la responsabilidad civil que un indebido manejo de datos personales pueda ocasionar.

El campo de protección debe ser también amplio, ya que los medios electrónicos invaden aspectos tales como domicilio, número telefónico, ocupación, preferencia sexual, salud, todo tipo de información que pueda afectar la esfera de privacidad de un individuo.

Las empresas que usen o más aún que comercialicen este tipo de información deben estar reguladas y supervisadas por órganos gubernamentales para efecto de prohibir la comercialización, sería ir en contra del mercado y el avance tecnológico impedir esa situación.

Por eso, sólo nos queda legislar sobre la materia para lograr establecer un equilibrio justo entre los intereses individuales, las necesidades del Estado y los requerimientos de un mercado en continúa expansión.

Necesitamos todo un marco jurídico incluyente que involucre a los sectores público, privado y social en la protección de datos personales, donde se garantice la protección de la privacidad sin descuidar los aspectos económicos, tecnológicos, de mercado que han detonado la expansión de esta actividad.

Ahora estamos en una época de efervescencia electoral, no escapa a nuestra atención la protección que se debe dar a los datos personales del electorado, frente al legítimo interés de los partidos políticos de promover el voto.

La tecnología y los usos comerciales de las grandes bases de datos no pueden ser contenidas, por ello una legislación en esta materia es apremiante, se deben fijar las reglas que determinen lo permisible de aquellas conductas que lesionen la esfera de intimidad de los particulares.

La Universidad Anáhuac y su Facultad de Derecho se suman a sus esfuerzos, a los esfuerzos del Instituto Federal de Acceso a la Información Pública, a los del Instituto de Transparencia y Acceso a la Información del Estado de México, a la Legislatura del Estado de México en el sentido de promover la discusión, análisis y reflexión en torno a este trascendente tema.

Son las universidades, las que desde un punto de vista objetivo e imparcial pueden orientar el trabajo de los legisladores federales y locales y de las autoridades encargadas de hacer cumplir la ley.

En suma, es la academia que engloba todas las corrientes del pensamiento, y se ubica por encima de las corrientes políticas, de las divergencias políticas, la que debe encauzar el debate abierto e incluyente sobre este tema.

Este tema provocará continuos debates y se proyecta como un tema de relevancia para el presente y el futuro. Un futuro en el que nosotros podemos incidir. Un futuro que nos pertenece, y que será mejor en la medida en la que cada uno

de nosotros cumpla su misión, y nuestra Facultad de Derecho consolide su posición de liderazgo en la formación de juristas y profesionales de excelencia. Así lo demanda México, y en ello nos comprometemos.

María Marván Laborde.

Agradezco el honor que nos hace la Red a México, de pedirnos que nosotros hagamos la Declaración, y en nombre de mis compañeros leeré yo esta Declaración de México, y en nombre de toda la Red.

Declaración de México IV Encuentro Iberoamericano de Protección de Datos Personales, México 2005

Los miembros de la Red Iberoamérica de Protección de Datos reunidos en la Ciudad de México y en el Estado de México del 2 al 4 de noviembre de 2005, ponen de manifiesto su satisfacción por los desarrollos que han tenido durante la celebración de IV Encuentro Iberoamericano de Protección de Datos Personales, y desean hacer públicas las conclusiones que se han alcanzado en el mismo.

El Encuentro ha aportado dos novedades particularmente destacadas. En primer lugar, la apertura de su sesiones a la participación de asistentes que no están integrados en la Red Iberoamericana, el amplio número de personas que han acudido a los paneles del Encuentro acredita de forma indubitable la creciente sensibilidad e importancia de las cuestiones relacionadas con la protección de datos personales para un número creciente de personas y entidades públicas y privadas.

En segundo lugar, las conclusiones del Encuentro no se apoyan exclusivamente en los debates celebrados durante el mismo, sino que incorporan detallados documentos de trabajo, fruto de un análisis más exhaustivo de los temas abordados en el mismo.

Este hecho constituye un indicador de la Red Iberoamericana se encuentra en condiciones de abordar y ofrecer alternativas rigurosas a problemas que afectan a la protección de los datos personales.

En este sentido, constatan que las perspectivas recogidas en la *Declaración de Cartagena de Indias*, Colombia, relativas a que la Red Iberoamericana sea un punto de referencia, objetivo e imparcial, para la implantación efectiva del derecho fundamental a la protección de datos personales, son una realidad capaz de influir en la forma decisiva, en el desarrollo institucional, social y económico de los países iberoamericanos.

En consecuencia, teniendo en cuenta los paneles desarrollados y los documentos elaborados por los grupos de trabajo de la Red, hacen públicas las siguientes conclusiones de sus documentos anexos:

Primero. Derecho fundamental de la protección de datos personales

El derecho a la protección de datos personales presenta caracteres propios que le dotan de una naturaleza autónoma, de tal forma que su contenido esencial le distingue de otros derechos fundamentales y específicamente del derecho a la intimidad, al honor y a la propia imagen.

El derecho a la intimidad tiende a caracterizarse como el derecho a ser dejado solo y a evitar injerencias en la vida privada.

El derecho a la protección de datos atribuye a la persona un poder de disposición y control sobre los datos que le conciernen, partiendo del

reconocimiento de que tales datos van a ser objeto de tratamiento, corresponsables públicos.

Dicho tratamiento impone a los responsables una obligación positiva al objeto de que se lleve a cabo, con pleno respeto al sistema de garantías propio de este derecho fundamental.

En ocasiones se ha planteado que el derecho a la protección de datos constituye una barrera para la tutela de otros derechos fundamentales o intereses públicas tutelables, como la libertad de información, la transparencia y el acceso a la información, que obre en poder de entidades públicas o el desarrollo de la actividad económica.

Frente a estas afirmaciones debe destacarse que no se producen propiamente conflictos entre unos y otros, sino más bien puntos de contacto cuya resolución se encuentra en la búsqueda de puntos de equilibrio que hagan compatibles a unos y a otros.

Sin embargo, no puede olvidarse que sólo respetando el derecho fundamental de todos a la protección de sus datos personales, se conseguirá un marco adecuado de respeto a la libertad de expresión y al acceso a la información y un correcto desarrollo del mercado.

En particular los elementos que permiten alcanzar un punto de equilibrio entre la protección de los datos personales y el acceso a la información pública, se contemplan específicamente en uno de los documentos anexos a esta Declaración.

Segundo. Las nuevas exigencias de las tecnologías de información

La *Declaración de Cartagena de Indias*, aportó una primera consideración sobre la incidencia que supone para la protección de datos personales, su tratamiento en el sector de las telecomunicaciones e Internet, con una referencia específica a los problemas que plantean las comunicaciones electrónicas o mensajes de datos, no consentidos ni deseados, popularmente conocidos como Spam.

En dicha Declaración se partía de la premisa de que el desarrollo de las telecomunicaciones y de los servicios de las sociedades de información, suponen necesariamente el tratamiento de datos de carácter personal y la necesidad de adaptar las garantías propias del derecho fundamental que los protege, a las circunstancias específicas de dichos tratamientos

Esta perspectiva ha confluido con la necesidad de construir la sociedad de información y del conocimiento, como un desafío global para el nuevo milenio, en los términos recogidos en la *Declaración de Principios de la Cumbre Mundial*, celebrada en Ginebra, en el año de 2003, cuya continuación tendrá lugar en Túnez, en 2005.

La conexión entre ambas perspectivas ha sido objeto de una declaración expresa en la Conferencia Internacional de Comisarios de Protección de Datos y de la Privacidad, que tuvo lugar del 13 al 15 de septiembre de 2005, en Montreux, Suiza.

La Declaración de Principios, entre otros aspectos, reconoció que las tecnologías de la información y las comunicaciones deben jugar un papel destacado en el desarrollo de la educación, la información y el conocimiento y posibilitan el crecimiento económico, como consecuencia de las mejoras que pueden suponer para alcanzar una mayor eficiencia y productividad.

Para conseguirlo, la Declaración enumera diversas necesidades entre las que se incluye como requisito previo, la de fomentar la confianza y seguridad de los usuarios y la de hacer frente al fenómeno del Spam.

Para ello, la declaración considera insoslayable la existencia de un marco jurídico y transparente, competitivo, tecnológicamente neutro, predecible y adaptado a las necesidades nacionales.

Desde la perspectiva de la protección de dato, la articulación de este marco jurídico debe asumir,

como criterios, la neutralidad tecnológica que permite a las garantías inherentes aquella protección opere con independencia de la tecnología utilizada, así como la articulación de estas garantías como derechos subjetivos de los abonados y de los usuarios, de forma que puedan ejercitarse frente a cualquier tercero que los lesione.

Asimismo, debe considerarse la posibilidad de que tales garantías puedan amparar a las personas jurídicas o morales.

Por su parte la respuesta al fenómeno del Spam debe incluir un marco jurídico dotado de instrumentos para sancionarlo; la colaboración entre las autoridades competentes para aplicarlo, los prestadores de servicios y los usuarios la concienciación de éstos últimos y la cooperación internacional.

En el ámbito de los servicios de la sociedad de la información es necesario considerar adicionalmente, la necesidad de desarrollar instrumentos de forma electrónica, así como contemplar los problemas relacionados con la protección de los derechos de propiedad intelectual, de forma que resulte compatible con el derecho a la protección de datos personales.

El desarrollo de la sociedad de la información permite adicionalmente nuevas posibilidades para que las entidades públicas mejoren los servicios e información ofrecidas a los ciudadanos, aumente la eficiencia y la eficacia de la gestión pública e incrementen sustantivamente la transparencia del sector público, así como la participación de los ciudadanos. Para ello es preciso estimular la implantación de proyectos de gobierno electrónico que hagan posible la consecución de los objetivos citados con el derecho de las personas a la protección de sus datos.

El detalle de las implicaciones que plantea el tratamiento de datos personales en el sector de las telecomunicaciones y en la implementación del gobierno electrónico se recoge en el documento adjunto a la presente Declaración.

Tercero. Desarrollos normativos y globalización

En consideración a los debates que tuvieron lugar durante el III Encuentro Iberoamericano, la *Declaración de Cartagena de Indias* recogió diversas conclusiones respecto de las implicaciones que la protección de datos personales supone para otros ámbitos de la actividad económica, como son los del sector financiero, el sector comercial y el uso de la información con fines de marketing y la trasferencias internacionales de datos como elemento prescindible para el desarrollo del comercio en mercados regionales o en el mercado mundial.

Durante el IV Encuentro se han vuelto a analizar dichas implicaciones en los ámbitos mencionados, proyectando tales implicaciones al conjunto de de actividad económica. A este respecto se han puesto de manifiesto la necesidad de conjugar mecanismos de protección de datos que neutralicen los desafíos y riesgos que plantea la globalización, sin menoscabar el desarrollo económico, industrial y tecnológico de las sociedades.

En el marco de este análisis ha sido objeto de consideración especial la relacionada con los elementos que deben integrar el marco normativo adecuado para garantizar la protección de datos personales. En este sentido se ha considerado la relación que debe existir entre la posibilidad de que el Estado apruebe una regulación imperativa de carácter general o sectorial y las iniciativas de los propios operadores para que la protección de los datos personales se lleve a cabo a través de instrumentos de autorregulación.

La opción por esta última alternativa como instrumento exclusivo para alcanzar un adecuado equilibrio entre las necesidades de los operadores económicos para desarrollar su actividad y la protección de datos de las personas debe ser descartada por cuanto constituye un sistema de protección jurídica inadecuado para la tutela de un derecho fundamental, al quedar

éste únicamente supeditado a la decisión de las entidades afectas, excluyendo la intervención de los poderes públicos.

Sin embargo, ello no significa que deba descartarse las iniciativas de autorregulación con carácter complementario a un marco normativo previamente definido por el Estado, en efecto, los instrumentos de autorregulación pueden ofrecer un valor añadido a la protección de datos personales, bien porque la iniciativa empresarial pretenda significarse con un elemento de mayor calidad en el trato de los datos de sus clientes ante la insuficiencia de las regulaciones aprobadas por el Estado o añadiendo garantías adicionales a las contempladas en tales regulaciones.

Bien porque permitan adaptar normativas sectoriales a las especificidades que presenta el tratamiento de datos en un determinado sector de actividad, de forma que se generen estándares que faciliten su cumplimiento adaptados a las necesidades del sector.

Cuarto. Los datos de salud

Como datos especialmente protegidos y su seguridad, los denominados datos especialmente protegidos deben ser objeto de una consideración específica por cuanto que dentro del marco regulador de la protección de datos personales exigen instrumentos adicionales de garantía.
Una primera reflexión que suscitan los datos especialmente protegidos es la que afecta su propia delimitación cerrada o abierta por medio de una numeración meramente ejemplificativa.

Sin embargo, no cabe duda de que en todo caso deben ser incluidos en esta categoría los datos relativos a la salud de las personas.

El tratamiento de los datos de salud necesita de una delimitación previa, dirigida a delimitar su concepto y si ha de ser objeto de una interpretación expansiva o restrictiva.

Tanto este análisis, como el relacionado a la legitimación de su tratamiento y el acceso a los datos de salud, debe partir de una interpretación armónica de la normativa de la protección de datos y las regulaciones sectoriales en el ámbito de la sanidad.

De este modo será posible alcanzar soluciones de equilibrio respecto a la titularidad de la información clínica, a las finalidades que justifican el acceso y uso de la misma, a las obligaciones de conservarla y a las medidas de seguridad y al secreto.

Estas soluciones deberán tener en cuenta no sólo el derecho fundamental de la persona a la protección de los datos personales, sino también la necesidad de permitir la definición de las políticas públicas que atendiendo a la consecución de intereses generales implican el acceso y tratamiento de los datos de salud, incluso relacionada con otros datos especialmente protegidos, como son los de origen racial o étnico y de vida sexual.

Quinto. La Declaración de la 12 Cumbre Iberoamericana de Jefes de Estado y de Gobierno, celebrada en Santa Cruz de la Sierra, asumió, entre otros aspectos, que la protección de los datos personales es un derecho fundamental de las personas; destacó la importancia de las iniciativas regulatorias Iberoamericanas para proteger la privacidad de los ciudadanos y reconoció formalmente el papel positivo que la Red Iberoamericana de Protección de Datos personales debe ocupar en la consecución de dichas finalidades.

La *Declaración de Cartagena de Indias*, supuso una concreción a los pasos a desarrollarse para la consecución de sus objetivos, defendiendo como primeras actuaciones la definición de una estrategia de la red y el análisis sobre la viabilidad de creación de autoridades de control en el entorno Iberoamericano. Ambas tareas han sido cumplidas recogiéndose sus análisis y conclusiones en los oportunos documentos anexos a esta declaración.

Sexto. El IV Encuentro Iberoamericano de Protección de Datos personales ha coincido felizmente con las ultimas fases del proceso legislativo parlamentario de la iniciativa de la Ley Federal de Protección de Datos Personales.

México se encuentra inmerso en un proceso legislativo de discusión a efecto de generar un marco jurídico aplicable a la protección de datos personales, para ello el proceso correspondiente debe tomar en consideración la experiencia internacional adquirida en la materia y permitir un equilibrio eficaz entre el flujo regulado y necesario de la información para promover los mercados en constante desarrollo y expansión y la protección de datos de la persona en el ámbito de la protección de datos.

Adicionalmente es imperativo que esta ley promueva la cultura de la protección de datos entre los individuos, de forma tal que la misma se convierta en un valor fundamental en nuestra sociedad.

Así, una Ley de Protección de Datos Personales en México debería considerar los principios de protección de datos personales internacionalmente reconocidos y aplicables tanto a las entidades públicas, como privadas.

Por otro lado, debe adecuarse a las condiciones sociales, políticas y económicas del país, estableciendo al mismo tiempo reglas claras y sencillas que permitan no sólo su implementación y cumplimiento, sino también un equilibrio entre el flujo de datos personales y su protección.

Por último, la ley debe garantizar el ejercicio efectivo del derecho a la protección de datos de las personas, y promover una cultura de confianza y respeto a los derechos humanos a través de instituciones independientes.

La Red Iberoamericana se congratula de la iniciativa mexicana en el convencimiento de que supondrá un nuevo impulso para garantizar la protección de datos personales en la región.

Séptimo. La Red Iberoamericana de Protección de Datos se congratula y felicita cordialmente a la Dirección Nacional de Protección de Datos de la República Argentina, por haber asumido la importante responsabilidad de organizar la XXVIII Conferencia Internacional de Comisionados de Protección de Datos y de la Privacidad, que tendrá lugar en Buenos Aires en noviembre del 2006.

La celebración de este evento es, sin duda, un reconocimiento internacional de la intensa actividad desarrollada por dicha Dirección Nacional en la garantía del derecho fundamental a la protección de datos personales y supondrá, sin duda, un nuevo impulso para su desarrollo en los países iberoamericanos.

Cierre de los trabajos del IV Encuentro Iberoamericano de Protección de Datos Personales

Juan Rodolfo Sánchez Gómez.

Se ha dicho que debe conciliarse el derecho a la protección de datos con otros derechos e intereses entre ellos, sin duda, el derecho a comer, el derecho a descansar, el derecho al ocio, y el derecho para quienes venimos de fuera de México a disfrutar de México, por eso tan sólo les quiero una vez más agradecer también a ustedes el que aún a estas horas sigan acompañándonos, y resaltar que la Red está ya totalmente consolidada, que la Red es una realidad.

Qué se puede decir, sin duda alguna que la cultura de la protección de datos está siendo sometida a un impulso extraordinario en toda la comunidad iberoamericana de naciones.

Y que debemos tener muy en cuenta, es algo que con cierta frecuencia digo, me gusta mucho parafrasear a Benito Juárez, diciendo que "*el respeto al dato ajeno es la paz*". Eso es lo que se puede conseguir, sin duda, con una cultura consolidada de protección de datos personales.

Celebro el trabajo serio y comprometido de la Red Iberoamericana de Datos Personales, de la que México es integrante, en donde se cuenta con valiosa experiencia de diversos países que, sin duda alguna enriquece y orienta los esfuerzos en la región latinoamericana sobre el tema.

Asimismo, felicito a los organizadores de este IV Encuentro, al IFAI al ITAIPEM, y a la LV Legislatura del Estado de México por los esfuerzos realizados para el éxito de este evento y por poner en la agenda de discusión del tema, caracterizado por el alto nivel de los ponentes que participaron en cada una de las mesas.

Con su amplia experiencia permitieron que tanto la sociedad como las autoridades podamos entender los alcances y las implicaciones en torno a la protección de los datos personales, a partir de diversos puntos de vista y de distintas realidades nacionales.

Efectivamente, la protección de los datos personales es un derecho fundamental que debe ser garantizado por las legislaciones nacionales, para proteger la dignidad de la persona frente a los desafíos de la globalización, las nuevas tecnologías de la información y el desarrollo de las telecomunicaciones.

Por ello, es indispensable tomar las medidas necesarias en los ámbitos correspondientes, para garantizar este derecho, observando en todo momento los principios mínimos de consentimiento, información, calidad, finalidad, seguridad y control en el uso, tratamiento, conservación, y manejo de los datos personales.

En este sentido es necesaria la participación de todos los actores económicos, políticos y sociales para fomentar el debate y adoptar una legislación acorde a la realidad de cada país y dar mayor seguridad en los procesos de intercambio transnacional de tipo financiero y comercial, respetando la integridad de la persona.

Sin duda, todo ello contribuye al fortalecimiento de la democracia en la región latinoamericana y de nuestro país en donde la protección y garantía de los derechos fundamentales no están sólo plasmados en un papel, si no que son una realidad.


IV Encuentro
Iberoamericano
de Protección de
Datos Personales

Esta Memoria del IV Encuentro Iberoamericano de Datos Personales México 2005
se terminó de imprimir
en el mes de noviembre de 2006
Tiraje: 2,500 ejemplares

Edición a cargo de:
Instituto Federal de Acceso a la Información Pública
(IFAI)

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

ifai
Instituto Federal de Acceso a la Información Pública

ITAIPEM