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.