Presentación del Libro: Privacidad y Derechos Humanos 2005

Presentador: Vamos a continuar con la presentación del libro que se refiere a la protección de datos de carácter personal en Iberoamérica, le doy la palabra al doctor José Luis Piñar Mañas.

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

En lo que a mí me atañe y como Presidente de la Red Iberoamericana de Protección de Datos, es un enorme honor y una gran satisfacción poder presentar hoy ante todos ustedes y en el marco del VI Encuentro Iberoamericano de Protección de Datos una publicación que es fruto del trabajo de la Red Iberoamericana de Protección de Datos.

La Red Iberoamericana de Protección de Datos surge en el año 2003, en la ciudad de La Antigua, en Guatemala. Allá se celebra un Encuentro de Protección de Datos Personales los días 2 a 6 de junio de 2003. Encuentro del que surge una declaración, la llamada *Declaración de La Antigua*, que consta de nueve puntos, uno de los cuales, el punto número siete es precisamente el de la creación de la Red Iberoamericana de Protección de Datos.

Y en ese punto, en el punto número siete, entre los compromisos que asume, los cometidos que asume la red, se encuentra el de promover la edición y publicación de documentos de trabajo y de las obras que permitan difundir y dar a conocer los resultados obtenidos en el desarrollo de las actividades de la Red Iberoamericana de Protección de Datos.

De la letra de la declaración pasamos a la acción y esa acción se ha concretado en la obra que hoy tenemos el gusto de presentar ante todos ustedes.

Se trata, en efecto del libro *Protección de Datos de Carácter personal en Iberoamérica*, que ha sido editado por la propia Red Iberoamericana de Protección de Datos, junto con la Agencia Española de Protección de Datos y una de las más prestigiosas editoriales jurídicas de España, la editorial Tirant lo blanch.

Este libro, del que tienen ustedes aquí algunos ejemplares, recoge los trabajos del encuentro al que antes me refería, el Encuentro celebrado en La Antigua, Guatemala, en junio del 2003.

Es una obra que pretende hacer ver que la red no sólo se manifiesta a través de declaraciones, a través de trabajos de enorme importancia, a través de la vía de fomentar, dar a conocer el derecho fundamental a la protección de datos personales, sino también a través de obras concretas, que

permitan a todos aquellos que quieren acercarse al derecho fundamental, a la protección de datos, tener un instrumento de información que les permita conocer la situación que en la materia se da en diversos países.

Este libro consta de dos partes bien diferenciadas. La primera está dedicada a lo que hemos denominado estudios generales; la segunda, la que se dedica a estudios nacionales.

Dentro de los estudios generales hay diversos trabajos que se refieren a cuestiones de carácter general, que tienen que ver con el derecho fundamental a la protección de datos.

Y en este sentido se abre con un trabajo de quien les habla, sobre el derecho fundamental a la protección de datos; a continuación un estudio sobre la evolución histórica y el marco normativo internacional del derecho fundamental a la protección de datos.

A continuación un trabajo de don Fernando Argüello, quien ha intervenido en este Encuentro, sobre protección de datos personales, *La Directiva Comunitaria, su influencia y repercusiones en Latinoamérica*.

Seguido de un estudio del doctor Juan Antonio Travieso, que también ayer tuvo ocasión de dirigirse a todos ustedes, sobre la protección de los datos personales en América Latina: *Unidos o Desprotegidos hacia una Red Iberoamericana de Datos Personales*.

A continuación un trabajo de don Jesús Rubí Navarrete, también ayer tuvo ocasión de intervenir en este Encuentro sobre *Tratamiento de datos personales en la prestación de servicios de telecomunicaciones*.

Otro más de don Emilio Aced, sobre transferencias internacionales de datos, y dos más en particular sobre cuestiones de carácter general, por más vinculadas al área iberoamericana y América Latina.

Por un lado un *Estudio sobre la conferencia iberoamericana, su sistema de cooperación y la protección de datos personales* y otro sobre *MERCOSUR y la protección de datos*.

Esta primera parte, por tanto, configura lo que sería los contenidos generales de la protección de datos personales.

La segunda parte se refiere, o se dedica a estudios nacionales, estudios de Colombia, a cargo del doctor Nelson Remolina; de la República de Costa Rica, a cargo del doctor Alfredo Chirino, también ha intervenido en este Encuentro y del doctor Mario Carbajal, que también nos acompaña, así como de don José Francisco Bart.

Estudios también de España, a cargo de Mar Martínez y de don Álvaro Canales.

También dos estudios de la situación en protección de datos en México, uno de ellos precisamente sobre el proyecto de Ley Federal de Protección de Datos Personales, redactado por el senador Antonio García Torres, quien es un miembro muy activo de la Red Iberoamericana de Protección de Datos, y otro sobre la legislación sobre protección de datos personales en México, redactado por don Eduardo Guerrero Gutiérrez.

Hay también un estudio sobre Paraguay, que se encargó de elaborar la Superintendencia de Bancos de Paraguay. Otro sobre Perú, elaborado por la doctora Lilián Oliver, y dos más sobre Uruguay, uno de ellos elaborado, redactado por el entonces senador, doctor Alberto Brause, y otro por la doctora Ana Brian, que también interviene en este Encuentro Iberoamericano de Protección de Datos.

Creemos que es una primera muestra de lo que quiere ser la Red Iberoamericana de Protección de Datos, un foro de encuentro, de intercambio de experiencias, de intercambio de información, que pretende facilitar la información a todos cuantos se mueven en el sector de la protección de datos, ya hemos dicho innumerables veces durante este Encuentro de un derecho

fundamental de todos y cada uno de los ciudadanos.

Junto a este libro querría también hacer una brevísima referencia a otra mucho más modesta, pero no por ella menos importante publicación de la red, que es la que contiene las declaraciones hasta ahora aprobadas en el marco de la Red Iberoamericana de Protección de Datos, y que se les han entregado a ustedes como parte de la documentación de este Encuentro.

La primera de ellas, de enorme importancia es la que tuvo lugar con ocasión de la Declaración de Santa Cruz de la Sierra, en la Decimotercera Cumbre Iberoamericana de Jefes de Estado y de Gobierno de noviembre de 2003, en la que se hace una referencia expresa en el punto 45 a la protección de datos personales y a la Red.

Permítanme muy brevemente leer este punto 45, que considero de enorme importancia:

Dicen unánimemente todos los jefes de estado y de gobierno de los 21 países iberoamericanos reunidos en Santa Cruz de la Sierra en Bolivia.

Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos, contenidas en la declaración de la Antigua por la que se crea la Red Iberoamericana de Protección de Datos abierta a todos los países de nuestra comunidad.

Por tanto reconocimiento expreso de que la protección de datos es un derecho fundamental. Reconocimiento expreso también de la importancia de la Red Iberoamericana de Protección de Datos.
Además, se recoge la declaración de la Antigua a la que antes me refería y también la declaración de Cartagena de Indias con motivo del encuentro celebrado en mayo de 2004, que recoge las conclusiones que entonces se alcanzaron en la Red referidas a temas de enorme importancia en nuestra opinión.

La primera de ellas sobre *La protección de datos y la perspectiva del sector financiero*.

La segunda. *La lucha contra el Spam*.

La tercera. *Las transferencias internacionales de datos, perspectivas Europea e Iberoamericana*.

La cuarta. *El sector de las telecomunicaciones e Internet ante los ataques de la privacidad*.

La quinta. *El sector comercial y el uso de la información con fines de marketing*.

La sexta. *Consideraciones en torno al desarrollo de la Red Iberoamericana de Protección de Datos*.

Es intención de la Red el acometer de inmediato la publicación, no sólo de estas declaraciones, sino también de la que surja de este encuentro, del Encuentro México 2005, al objeto de completar de este modo una publicación de mayor alcance incorporando todos los documentos que hasta ahora se han producido en el ámbito de la Red, no sólo en texto español, sino también traducidos al inglés para dar una mayor difusión a todo lo que en materia de protección de datos se está haciendo en el ámbito de la comunidad iberoamericana.

Tan sólo me resta agradecer muy de veras a todos cuantos han participado en la redacción de este libro y de estos documentos, por su tesón, por su infatigable labor, por su impulso y por su ánimo, desde que en junio del 2003 en una reunión que debo decir entonces era sumamente sencilla, me atrevería a decir, una reunión de no muchas personas que creíamos que había que dar una expresión de apoyo a todo cuanto se está haciendo mucho y bien en materia de de protección de datos en Iberoamérica, de una expresión del grupo que entonces surgió a lo que es este IV Encuentro Iberoamericano de Protección de Datos.

Agradecimiento a los que han colaborado en la Red, los que están colaborando en la Red. Agradecimiento a todos los que han participado

como autores del libro que ahora tengo el honor de presentar.

Y por último, y por supuesto agradecimiento a quienes han organizado, al IFAI sobre todo por habernos permitido presentar este libro en este Encuentro.

Y agradecimiento una vez más a todos ustedes. Tan solo decirles que disponemos de algunos ejemplares, pocos, pero quien tenga interés en esta obra, puede ponerse en contacto o bien con el IFAI o bien con la Agencia Española de Protección de Datos Personales.

Cédric Laurant: Consejero de Política, Director, Proyecto de Privacidad Internacional, Electronic Privacy Information Center-EPIC.

Les presentaré el libro y voy a hablar sobre los desarrollos globales que se llevaron a cabo en el período en que este libro se hizo desde junio del 2004 hasta julio del 2005.

Este libro proporciona una visión general del los temas más importantes de privacidad, desde la supervisión de satélites, del comercio, etc., y también revisa el estado de privacidad en más de 70 países en todo el mundo.

En la primera parte que se llama *Visión Global* que nos habla sobre lo básico de lo que es la privacidad, de lo que quiere decir privacidad e instituciones de protección, de cómo definir la privacidad, cuáles son los modelos de protección de privacidad.

Existen secciones que nos hablan sobre la vigilancia, la vigilancia de la comunicación, el consenso, la privacidad, la privacidad de los viajes, etc.

Y también hay una tercera parte sobre los informes de los 73 países que hemos analizado este año y en estos informes nosotros hemos tratado de dar una presentación, una introducción sobre el marco constitucional que se refiere a la privacidad a la protección de los datos y de la privacidad de las leyes criminalísticas y las de procesamiento criminal y también en los países donde dichas autoridades existen.

Y también incluimos algunos países como Nueva Zelanda que han ratificado en la Comisión Internacional los derechos de privacidad.

En este año también tuvimos una organización que incluida puntos muy breves sobre los desarrollos más importantes en esos países, las gráficas que incluyen las leyes de protección de privacidad en cada uno de los países, un glosario de recursos de privacidad internacional, que se pueden encontrar en diversos países, si ustedes quieren investigar más y cuáles son las informaciones que ya existen, las informaciones que hay en el libro. Y también tenemos una versión en CD.

Para la elaboración de este libro nosotros trabajamos con más de 200 expertos, desde profesores, académicos y autoridades de protección de datos, funcionarios del gobierno, activistas de derechos humanos, activistas diversos y personal diverso.

También les voy a hablar sobre lo que yo creo es lo más importante o el desarrollo más importante que se llevó a cabo en los últimos 12 meses.

Esta investigación más bien se enfoca en la supervisión del gobierno y en las acciones gubernamentales, en la privacidad de cómo responder ante la amenaza del terrorismo.

Primero vamos a hablar de uno de los desarrollos más importantes que son las medidas que el gobierno tomó y realizó para responder frente a terrorismo y también de otras medidas gubernamentales de bases de datos de información de salud y de uno de los desarrollos más importantes en los últimos 12 meses en el campo de supervisión de privacidad y de identificación y tecnología de frecuencias de radio.

También hay un cuarto punto al respecto, y quisiera hablar de las leyes de protección de datos en diversos países, de las tendencias de privacidad y sobre los retos más importantes de la privacidad futura.

Lo que hemos encontrado en EPIC, al trabajar en este estudio es que no ha habido muchos cambios en los últimos tres o cuatro años, en especial desde septiembre del 2001 con los ataques terroristas en los Estados Unidos, en Madrid, en Indonesia, en Londres, y también en la forma en que el gobierno ha tratado de responder a la amenaza del terrorismo y también a la forma en que han tratado o han implementado dichas leyes.

Primero parecía que las leyes que se habían puesto en vigor tenían el propósito legítimo y más adelante lo que sucedió fue que una vez que este marco legal ya estaba en vigor, había dado toda la disposición de nuevos poderes a las autoridades de aplicación de la ley y estas leyes se extendieron o estos poderes que se les dieron a las autoridades, de aplicación de la ley, se les dieron de una manera para luchar contra el terrorismo y en contra de otras amenazas, no solamente del terrorismo, sino de otros actos criminales.

Lo que descubrimos en los últimos tres o cuatro años, fue que los países han añadido mucho más de agencias gubernamentales y departamentos gubernamentales, que tienen que ver específicamente con las tareas de luchar contra el terrorismo y de recopilar datos, de coordinar y de compartir información.

Y también hay una retención de los datos, en especial en Europa, pero también en algunos países africanos y latinoamericanos, al igual que la tendencia para centralizar los datos.

Esa no es diapositiva correcta, sino la 1.2, es la siguiente.

Otra tendencia que encontramos es que los gobiernos están dispuestos, con tal de proteger las fronteras, con tal de proteger los medios de transportes, a identificar a las personas en las fronteras.

Primero empezó en las fronteras y después con las revisiones domésticas. Entonces, en principio los países presentaron la idea de supervisar a los pasajeros, de sacarles un perfil y uno de los sistemas más notorios es el sistema estadounidense de seguridad del transporte o sistema de computadora que es como pasar por la pantalla a los pasajeros y EPIC y otros grupos en los Estados Unidos empezaron denunciarlo.

Sin embargo, fue reemplazado adecuadamente por otro sistema y fue una situación que otros países siguieron: Canadá, Australia, la Unión Europea y también algunos países asiáticos.

Lo que yo creo que son los principales asuntos de protección de datos en el caso de este nuevo poder de prescribir un perfil, dado que estas autoridades de aplicación de la ley es el hecho de que más específicamente en el caso de los Estados Unidos, violó las leyes de protección de los datos europeos.

Y, otro caso, que sucedió es que el Gobierno americano protegía sus fronteras y trataba de obtener información a partir de compañías privadas de los Estados Unidos sobre los ciudadanos que vivían, en por lo menos 10 países de Latinoamérica, la información había sido conseguida de una manera ilegal.

Y lo que ocurrió es que la autoridad en los Estados Unidos tomó información de esta compañía privada, compañía local en Brasil, Colombia y México, con tal de ver si había un enfrentamiento entre lo que los inmigrantes habían dicho a estas autoridades fronterizas y lo que los Estados Unidos tenían en sus archivos.

Otra tendencia preocupante es el hecho de que los datos una vez obtenidos por las autoridades de aplicación de la ley y algunas veces la violación de estos datos de protección nacional no está segura de no ser transferida hacia otra

autoridad de aplicación de la ley, que no estaba de acuerdo con esta ley de protección de datos en vigor.

Una situación muy notoria fue la que se llevó a cabo en los Estados Unidos, se llamaba "las visitas de los Estados Unidos", que obligan a todas las personas que entren a los Estados Unidos a dar sus huellas digitales y tomarle una fotografía para poder formar un sistema indicando la identidad de la persona que entra al país.

Específicamente este año nosotros vemos que la mayoría de los países que hemos analizado han salido con ideas o han tenido ideas para cartas inteligentes o tarjetas inteligentes con un número único de identificación, como licencia de manejo, una especie de CURP, huellas digitales, piel, etcétera.

Los principales problemas relacionados con esta presentación de tarjetas inteligentes es que la mayoría de los países que los presentaron no tienen una forma de protección. Eso significa que ellos dan más poderes a las autoridades de aplicación de la ley, sin darles la situación adecuada a otras agencias gubernamentales o grupos de protección al consumidor que tienen la situaron de poder ver si estos poderes que les otorgan los utilizan de una manera adecuada.

Otras medidas gubernamentales que vemos específicamente es la presentación de esta información en la base de datos.

Ya había esta información, pero vemos que cada vez más gobiernos utilizan esta base de datos para poder combatir el terrorismo, y en los países que no tienen esa protección de datos se hace para estos problemas, porque ayuda a que la información médica sea muy sensible a los datos personales, y confía o depende únicamente del gobierno para tratar con esta información, sin abusar de ella y sin diseminarla.

Los poderes adecuados que generalmente no se pueden llevar a cabo, en la mayoría de los países y en especial en los Estados Unidos, lo vimos en muchos casos en donde la información está recolectada por compañías privadas.

Ahora, esto está sin que haya salvaguardas establecidas para poder supervisar las prácticas gubernamentales.

En el campo de lo que es la supervisión del sector privado, una de las tendencias más importantes es el uso de lo que se llama RFID (Identificación de Radio Frecuencia). Esta tecnología realmente no es nueva y se comenzó a utilizar hace como 15 ó 20 años e incluso más en los años 60, pero ahora por el precio tan disminuido de la tecnología y el tamaño tan disminuido de los detectores, hemos visto muchas más aplicaciones que han surgido en lo que es la industria de la defensa.

Se están utilizando detectores de radiofrecuencia para monitorear a los empleados en los lugares de trabajo, para monitorear a los niños en las escuelas, para monitorear a la gente en los hoteles y muchas de estas aplicaciones tienen un rango de precios. Por ejemplo, cuando se tuvo un sistema en Malasia, es una tarjeta inteligente con identificación de radio frecuencia, ésta tenía mucha información sobre la persona y se encontraba en una tarjeta; la de la licencia de manejo, los registros médicos, mucha información.

Lo que está sucediendo más bien, la información de la tarjeta se está centralizando y era muy interesante para *hackers* y gente que roba la identidad.

Quisiera decir que la tecnología de RFID vemos muchas cosas nuevas, lo que son lineamientos, leyes, reglamentos que están trabajando en este campo.

Y también en otros países en donde hay cada vez más industrias, compañías y gobiernos. Esto es un campo en que hay una vigilancia muy intensiva en lo que es la tecnología de identificación de radio frecuencia en la

información financiera y de transacciones, entre asociados, un producto por ejemplo que se compra en la tienda para ver la ubicación.

Lo que quiero decir aquí es que esto se podría utilizar posteriormente para otros propósitos que no están en el sistema de formación de perfiles, y lo que termina sucediendo es que la tecnología comienza con una meta legítima y termina siendo para prevenir cualquier tipo de crimen en un aeropuerto, por ejemplo en Estados Unidos.

Otra tendencia de privacidad es que las autoridades de aplicación de la ley están interesadas en recolectar toda la información que puedan y delegan esta recolección o esta tarea de procesamiento de información a las empresas privadas.

Hay casos muy famosos de los que quiero hablar que son, por ejemplo, una compañía estadounidense llamad Check Point que ayudó a los estadounidenses a obtener información que no podía obtener legalmente, obteniendo esta información de ciudadanos latinoamericanos y mandándola al gobierno. De esta manera se evitaba la aplicación de una ley en Estados Unidos que evitaba que el gobierno obtuviera estos datos.

También encontramos y es difícil llegar a esta conclusión, que la seguridad nacional normalmente se ha detenido por los derechos humanos y los derechos a la privacidad, también la conveniencia.

Un ejemplo, el Departamento de Estado de la Unión Americana, junto con el Ministerio de Relaciones Exteriores de México empezaron a utilizar la identificación de radiofrecuencia en los pasaportes, y aquí la razón principal para hacerlo era la propuesta inicial del Departamento de Estado que fue en diciembre de 2004 y enero de 2005, era poder acelerar el paso de la gente por las líneas fronterizas, aquí se puede ver el valor o la conveniencia que era mucho más importante que el derecho a la privacidad.

Por estas razones creo que los retos siguientes que veremos en la privacidad van a ser pensar cómo los gobiernos y la sociedad civil pudieran establecer unas salvaguardas y supervisiones seguras sobre el uso que está haciendo el gobierno de los nuevos poderes que está obteniendo.

Podemos pensar en las nuevas formas de obtener esta nueva protección con las leyes, esto es potencialmente tecnología muy intrusiva, por ejemplo, sale muy barato como un implante que una empresa pensó en utilizar, y esto indicaría en ponerlo en una persona en el antebrazo, cuando esta persona quedara inconsciente esto llamaría a los paramédicos y a los doctores y esto llevaría información médica del paciente en caso de que él no tuviera un estado adecuado para dar información.

Y en este caso específico, parte de la Unión Europea y algunos lineamientos en países asiáticos no tienen ningún marco de privacidad en vigor, por ejemplo, en Estados Unidos no hay ningún marco de privacidad que aborde estas amenazas de manera específica.

Otro reto de la privacidad sería ver qué es lo que sucede cuando la información que se recolectó de manera legítima y legal en un país tiene que transportarse a otro país, eso crea asuntos de las normas globales de privacidad o flujos transfronterizos de información y este es un gran debate ahora en Latinoamérica, esto se enfrenta con dos modelos básicos: Los modelos en la Unión Europea y el marco del área Asia Pacífico, en la parte cooperativa de Asia Pacífico.

Quisiera evitar los datos, vieran estos importes en las páginas Web en las siguientes semanas o en ésta, está disponible en inglés y a mediados de diciembre en español.

Pedro Mendizábal: Ciudadanía y Derechos en la sociedad de la información, CPSR-Perú.

Para CPSR-Perú es muy grato compartir la presentación en este foro de lo que será la primera edición en castellano del libro

Privacidad y Derechos Humanos, versión correspondiente al año 2005.

CPSR-Perú es un centro de investigación en políticas públicas y tecnologías de la información y comunicaciones, fundado en Lima en octubre de 2002, su misión consiste en promover el uso y desarrollo socialmente responsable de las tecnologías de la información; influenciar en las decisiones vinculadas con las mismas y fomentar el desarrollo de las sociedades de información que concilie la tecnología con el ser humano que la usa.

El campo de acción de CPSR-Perú se sitúa en aquel punto en que convergen tecnologías de la información, derecho y sociedad.

En tal sentido, tiene varias áreas de trabajo entre las que destacan las relativas a derecho de autor en el entorno digital, sociedad de la información, privacidad y protección de datos personales, seguridad de informática, de la información y comunicaciones, entre otras, todas ellas abordadas desde un enfoque interdisciplinario que involucra lo técnico, jurídico, económico, político, social, cultural y ético.

Desde el 28 de septiembre de 2005 CPSR-Perú ha sido incorporado a la Red Iberoamericana de Protección de Datos, como miembro asociado.

La intimidad personal, definida desde la óptica del sujeto que goza y ejerce su derecho, representa el ámbito de libertad del individuo, el momento y lugar en que, como decía Rousseau, lo íntimo de identifica con lo universal.

Ello le permite a la persona reencontrarse consigo misma, recargar energías para retornar con brío a las actividades sociales, en especial trabajo. Es, asimismo, el espacio de sosiego en que toma decisiones que afectarán su futuro y que tendrán, en la sumatoria de millones de intimidades y autonomías, consecuencias de amplios alcances.

La intimidad, pensada desde el individuo hacia el mundo exterior, entendida como espacio de libertad, en el que el sujeto decide en qué medida expone o no su vida privada, disminuye apreciaciones negativas del derecho a la intimidad que lo vinculan, en ocasiones, con el secretismo o individualismo.

Concebido desde esta perspectiva, el derecho a la intimidad se revela no como el derecho del solitario o del ermitaño, sino como el ejercicio de la mínima y necesaria libertad y autonomía que el derecho moderno debe garantizar a la persona humana, para que a partir de su personalidad en acción edifique o público y social.

Por ende, estamos ante un derecho fundamental base de la ciudadanía y dinámicamente relacionado con aquella noción clásica, según la cual el ser humano es ser humano en sociedad.

Lo planteado justifica el esfuerzo por averiguar en 73 países, convocando la participación de más de 200 expertos y colaboradores, durante casi un año de labores, cuál es el estado de la privacidad en el planeta.

La edición en castellano contendrá la parte general del PHR 2005, los reportes individuales de 14 países de América Latina, los capítulos referentes a aquellas legislaciones más influyentes en nuestro medio, como son España, Portugal, Italia, Francia, Alemania y la Unión Europea.

Por relevancia y contraste se ha decidido incluir los reportes de los Estados Unidos, Gran Bretaña y Canadá.

Ahora bien, hemos comenzado refiriéndonos a la intimidad personal y familiar. ¿Cómo se explica, entonces, que el libro que ahora presentamos posea contenidos que exceden largamente el derecho a la intimidad?

Por ejemplo, temas referidos a identidad personal, votación electrónica, privacidad respeto de los datos de viaje, nanotecnología, acceso a la información pública, entre otros.

Interpretado en términos de la tradición jurídica romano germánica, el concepto del *right of privacy* y del *common law*, comprende al menos el derecho a la intimidad personal y familiar propiamente dicho, el secreto de las comunicaciones y la confidencialidad de los documentos privados; la privacidad genética, la privacidad física frente a procedimientos tales como la biometría, el auscultamiento de cavidades corporales, la inviolabilidad del domicilio, la privacidad en los lugares de trabajo e incluso en espacios públicos, así como todo aquello que de una u otra manera proteja la dignidad humana.

El *right of privacy* estadounidense corresponde más a la concepción alemana del derecho general de la personalidad.

El derecho general de la personalidad, entendido como derecho matriz que comprende una amplia gama de derechos innatos, vitalicios, personalísimos, extrapatrimoniales, relativamente indisponibles, nominados o innominados, contenidos o no en el derecho positivo, responde al espíritu garantista de protección de la persona como un todo. Hecha esta breve introducción pasemos a revisar someramente algunos de los resultados fruto de la investigación realizada en latinoamericana.

En la República Argentina, debido a la presión pública por un creciente número de secuestros, se promulgó en mayo de 2004 una ley sobre los servicios de comunicaciones móviles, que eliminó el anonimato en la compra de celulares. La ley obliga a los que venden teléfonos móviles a recolectar la identidad de sus clientes, incluso de aquellos que tienen la modalidad de servicio con tarjeta prepago.

En enero de 2004 el Congreso aprobó la controvertida ley 25873, la misma que modificó la Ley Nacional de Telecomunicaciones de 2003, estableciendo la obligación de las empresas de telecomunicaciones de colaborar con las investigaciones de la justicia, y en concreto, con los pedidos de informes, así como con la obligación de retener ciertos datos de tráfico (telefónicos, por Internet y por cualquier otro medio como la telefonía IP) por el lapso de 10 años.

El reglamento de esta ley generó gran discusión pública. La cámara que agrupa las empresas de telecomunicaciones interpuso una acción de amparo en contra de la aplicación del decreto reglamentario, basándose en los costos que acarreaba el cumplimiento de la medida. Debido a la presión mediática el Presidente Kirchner suspendió el decreto que él mismo había expedido.

En Bolivia se agregó en el año 2004 la acción de Hábeas data al texto constitucional, la misma que se puede seguir mediante un proceso sumarísimo.

En Brasil se han presentado al Congreso varios proyectos de ley. Algunos de ellos obligarían a los proveedores de servicios de Internet y proveedores de alojamiento Web a mantener información personal identificable, tal como el nombre, número de documento de identidad, dirección y teléfono de los clientes, por un plazo de dos a cinco años, así como datos de tráfico de las conexiones individuales a la Internet, incluyendo los números IP de los emisores y receptores de las comunicaciones, cuando se conectan y desconectan a la Internet la cantidad de data enviada y recibida, por un lapso de seis meses a cinco años.

La intercepción ilegal de comunicaciones por parte de investigadores privados, así como la grabación de conversaciones privadas son fenómenos comunes en Brasil. También en 2004, como respuesta a escándalos que involucraban a funcionarios del gobierno federal, el Ministerio de Justicia manifestó su intención de presentar un proyecto de ley destinado a prohibir la intercepción y el uso de la información así recogida, con penas de cárcel para los periodistas que usen cualquier información obtenida a través de dichos medios.

Como reacción a las políticas antiterroristas de los Estados Unidos, que crearon un sistema de

registro de visitantes extranjeros, que comprende el fotografiado y la toma de huellas automatizadas; una corte brasileña resolvió, en reciprocidad, que los ciudadanos estadounidenses también tendrían que seguir similar procedimiento antes de permitírseles el ingreso a Brasil. No obstante la orden de la Corte fue luego revocada, un mecanismo similar fue establecido a través de un decreto del gobierno federal. Hacia finales de 2004, los gobiernos de Estados Unidos y Brasil acordaron mecanismos de cooperación recíprocos sobre la materia.

Respecto del creciente número de cámaras de video vigilancia en lugares públicos y privados, la ciudad de Sao Paulo promulgó una ordenanza municipal que ordena la instalación de signos distintivos, informando de la existencia de tales cámaras, tanto en lugares públicos como privadas. Las imágenes grabadas serán confidenciales, y el incumplimiento de las normas de protección de datos dará lugar a responsabilidad por parte de los infractores.

En Chile se aprobó una Ley de Protección al Consumidor que contiene disposiciones contra el Spam, establece un sistema opt-out y prescribe que todo correo electrónico comercial debe indicar el nombre del remitente, una descripción precisa de lo que ofrece y una dirección válida a la cual el consumidor pueda enviar un mensaje destinado a evitar cualquier futuro E-Mail.

En Colombia existen tres proyectos de *Hábeas data* en discusión, uno de los más controvertidos es el proyecto de ley estatutaria 071 de 2005, presentado por el Ministerio de Hacienda y algunos congresistas. Según el profesor Remolina dicho proyecto deteriora el alcance del derecho fundamental a la protección de los datos personales de los colombianos, fortalece a las empresas que negocian con dicha información y expone a Colombia a que sea catalogada internacionalmente como un país que no garantiza un nivel adecuado de protección a la información personal.

En Costa Rica hay tres proyectos de ley en discusión que regularían el procesamiento automatizado de información personal. La Corte Suprema ha reconocido el derecho a acceder a la información pública a pesar de no estar regulado.

En Ecuador se adoptó una Ley de Transparencia y Acceso a la Información Pública en mayo de 2004 que otorga a los ciudadanos el derecho a solicitar y obtener información sobre actos, contratos y proyectos firmados y financiados con recursos públicos. También en Ecuador se promulgó la Ley de los Burós de Información Crediticia que tiene como objeto regular la constitución, organización, funcionamiento y extinción de las centrales de riesgo. Según la norma legal, la información que obtengan y conserven tendrá por exclusiva finalidad el ser destinada a la prestación del servicio de referencias crediticias y deberá ser mantenida en el país. La información histórica de personas naturales y jurídicas no podrá exceder de seis años; por tanto, a los burós de información crediticia les está prohibido recabar y proporcionar informar posterior a ese límite.

En el Parlamento guatemalteco se presentó en febrero de 2005 un proyecto de ley de acceso a la información pública, clasificación y desclasificación de información en poder del Estado.

En México existen tres iniciativas legislativas referentes a protección de datos personales pendientes de aprobación. La ley mexicana de acceso a la información pública establece como uno de sus propósitos la protección de los datos personales contenidos en ficheros de entidades públicas; creó el Instituto Federal de Acceso a la Información Pública, uno de cuyos fines es la protección de tal información a través de la capacitación a los servidores públicos, la elaboración de estudios y procedimientos.

En el Perú se publicó en la página Web del Ministerio de Justicia, hacia agosto de 2004, un proyecto de ley de protección de datos

personales, que en líneas generales, sigue lo establecido en la normativa europea sobre la materia. Cabe destacar la promulgación en mayo de 2004 de la ley 28/2/37 Código Procesal Constitucional, que regula de manera integral los procesos constitucionales de *Hábeas corpus*, amparo, *Hábeas data*, cumplimiento, acción popular e inconstitucionalidad, sobre todo, porque se trató de una iniciativa privada impulsada de manera espontánea por un grupo de renombrados abogados peruanos que formularon un anteproyecto que con escasas modificaciones fue aprobado por el Congreso de la República.

En abril de 2005 se promulgó la ley que regula el uso del correo electrónico comercial no solicitado (Spam), la norma que se prevé que tendrá escaso efecto práctico establece que todo correo electrónico comercial, promocional o publicitario no solicitado, que se origine en el Perú, deberá contener características específicas de información, tales como la palabra *publicidad* en el asunto del mensaje, el nombre de la persona natural o jurídica que lo envía y una dirección de correo electrónica válida y activa que pueda ser utilizada para la exclusión voluntaria. La ley también dispone una compensación económica para las víctimas del Spam, obliga a los proveedores de servicios de Internet a contar con sistemas de filtro e inusitadamente los responsabiliza (siendo ellos también los afectados) por el Spam que reciban sus clientes.

En Venezuela se aprobó la Ley de Responsabilidad Social de la Radio y Televisión (RESORTE), denominada por la oposición la *ley mordaza*. En general esta ley establece franjas protegidas y programación de contenidos socialmente responsable. También regula la publicidad y prevé múltiples penas en caso de incumplimiento. Más allá de la justificación oficial de la norma como protectora de la población preventiva de la exposición de los niños y adolescentes a la información "inapropiada", la Sociedad Interamericana de Prensa y Reporteros sin Fronteras, han expresado su preocupación por la censura previa y restricciones a la información que la ley RESORTE establece.

En agosto de 2004 y en los meses siguientes la lista de quienes firmaron las planillas solicitando la revocatoria del mandato del presidente Chávez fue hecha pública en la Internet por el parlamentario Luis Tascón exponiéndolos a represalias de parte de seguidores del gobierno.

A manera de reflexión final y mirando el bosque, no sólo aquel grupo de árboles que conforman la jungla jurídica, en la sociedad de la información no son suficientes las normas legales, por más protectoras que ellas sean de los derechos de la persona humana, ni las autoridades de protección de datos, por más dignas e idóneas que sean del cargo que ocupan.

Es sencillo imaginar mil formas de transgredir las normas de protección de datos personales y lo que es peor, es igualmente fácil llevarlas a la práctica de manera impune.

Por lo tanto, si la *etérea composición* es insuficiente, si los procesos administrativos o jurisdiccionales son de probanza imposible, de desenlace incierto o resultado ilusorio, qué nos queda a los ciudadanos conscientes de la importancia de cautelar nuestra data. Pues debemos optar por la prevención y la defensa propia, prevención para no entregar data inconscientemente y sin razón suficiente y defensa propia mediante el uso de herramientas informáticas de auto-tutela o auto-composición que protegen nuestra privacidad y data personal.

Nos referimos, por ejemplo, al uso del correo electrónico seguro, herramientas de navegación anónimas en la Internet, el cifrado de las comunicaciones telefónicas y de los servicios de mensajería instantánea, así como bases de datos y discos duros encriptados.

Pensamos que es relevante que la Red Iberoamericana de Protección de Datos, debata

la posibilidad de ampliar la efectividad de su labor mediante el fomento del uso de este tipo de herramientas informáticas.

Es imperativo trabajar en educación para tener una ciudadanía concienciada y vigilante que premie a aquellos que cumplen con los principios de protección de datos de carácter personal y castigue a los que incumplen dichas normas.

Finalmente, lo más importante, educar en una ética que considere siempre al ser humano como un fin y nunca como un medio.

Agradecemos la cordial invitación del IFAI a la Red Iberoamericana de Protección de Datos y al Instituto de Transparencia y Acceso a la Información Pública del Estado de México por habernos permitido dirigirnos a ustedes.