Red Iberoamericana de Protección de Datos

VOLUMEN IV

TOMO 3

ifai

Instituto Federal de Acceso a la Información y Protección de Datos

LIBRO BLANCO
2006-2012

Volumen IV
Tomo 3

Índice

3.1 Presentación

La Red Iberoamericana de Protección de Datos (RIPD) se constituyó como una respuesta a la necesidad de fomentar, mantener y fortalecer un estrecho y constante intercambio de información, experiencias y conocimientos entre los países iberoamericanos, a través del diálogo y colaboración en materia de protección de datos de carácter personal. La RIPD se encuentra abierta a todos los países iberoamericanos que deseen promover y ejecutar iniciativas y proyectos relacionados con esta materia.

La Red no constituye un organismo internacional propiamente y no cuenta con personalidad jurídica propia. Tampoco está conformada por los representantes de los gobiernos de los países participantes, sino únicamente por quienes pertenecen a algún organismo público cuya actuación impacte sobre la protección de datos personales en sus respectivos países. Por ello, puede concluirse que la Red es un espacio para compartir experiencias e impulsar la adecuada protección del derecho cuidando el valor que brindan distintas perspectivas, con el ánimo de fortalecer coincidencias.

Entre los objetivos de la Red destaca especialmente su labor tendiente a impulsar la elaboración de los instrumentos normativos necesarios para garantizar este importante derecho fundamental en aquellos países de la comunidad iberoamericana en los que aún no se ha emprendido esta regulación.

La inclusión del IFAI a este foro le ha permitido compartir el conocimiento entre los países, las autoridades y las organizaciones de expertos en materia de privacidad. También le ha propiciado discutir cómo enfrentar de forma colectiva el avance de las nuevas tecnologías de la información que multiplican los riesgos para la vida privada de las personas.

El reporte de este libro incluye la participación del IFAI en la Red desde 2010 a la fecha, es decir, a partir del año de entrada en vigor en México de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la cual reconoce al Instituto Federal de Acceso a la Información y Protección de Datos, como autoridad garante en la materia, periodo que coincide con el tiempo que México lleva presidiendo este foro.

El IFAI, durante el ejercicio de la presidencia de la Red, ha promovido diversos seminarios y encuentros que se han realizado tanto en México como en otros países de la comunidad iberoamericana; estos espacios fortalecen la voluntad de servir de punto de encuentro para las iniciativas que desde los más diversos ámbitos regionales promuevan la protección de datos personales en un entorno global.

Alfonso Oñate Laborde
Secretario de Protección de Datos Personales

3.2 Antecedentes

La Red Iberoamericana de Protección de Datos (RIPD) surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, con la asistencia de representantes de 14 países.

La RIPD se constituyó como una respuesta a la necesidad de fomentar, mantener y fortalecer un estrecho y constante intercambio de información, experiencias y conocimientos entre los países iberoamericanos, a través del diálogo y colaboración en materia de protección de datos de carácter personal. La Red se encuentra abierta a todos los países de la región que deseen promover y ejecutar iniciativas y proyectos relacionados con esta materia.

Esta Red creó un foro integrador que permite la participación de diversos actores sociales, tanto del sector público como privado. Esta iniciativa contó desde sus inicios con el apoyo político de los participantes en la XIII Cumbre de Jefes de Estado y de Gobierno de los países iberoamericanos celebrada en Santa Cruz de la Sierra, Bolivia, 14 y 15 de noviembre de 2003, mismo que quedó plasmado en su Declaración Final en la que dan cuenta del carácter de la protección de datos personales como Derecho Fundamental, así como de la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos.

A partir de ese momento, la RIPD se convirtió en un foro de promoción del Derecho Fundamental a la protección de datos en esta comunidad, cuyo impulso y responsabilidad asumieron también los representantes políticos de los respectivos Estados signatarios de la Declaración de Santa Cruz de la Sierra.

La consolidación de este foro como cauce idóneo para la toma de decisiones, adopción de documentos y fijación de estrategias futuras se ha convertido en uno de los objetivos estratégicos de la RIPD. En definitiva, es interés primordial de las instituciones que en la actualidad la constituyen, el impulso e implantación del Derecho Fundamental a la Protección de Datos de Carácter Personal a través de las entidades con capacidad y competencias para instar a los gobiernos nacionales a que elaboren una regulación normativa en esta materia a efecto de lograr la obtención de la Declaración de Adecuación por parte de la Comisión Europea.

Los objetivos y la organización de la Red quedan recogidos en el Reglamento aprobado con motivo del VI Encuentro Iberoamericano de Protección de Datos, celebrado en Cartagena de Indias, Colombia, del 27 al 30 de mayo de 2008. [1]/

3.3 Marco Normativo

- Constitución Política de los Estados Unidos Mexicanos: artículos 6 y 16.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Las Leyes en la materia, expedidas por las entidades federativas.

[1] Anexo 1

3.4 Vinculación con el Plan Nacional de Desarrollo

El Plan Nacional de Desarrollo 2007-2012 está estructurado en cinco ejes rectores:

1. Estado de Derecho y seguridad.
2. Economía competitiva y generadora de empleos.
3. Igualdad de oportunidades.
4. Sustentabilidad ambiental.
5. Democracia efectiva y política exterior responsable.

El proyecto insignia "Red Iberoamericana de Protección de Datos" se inscribe en el quinto eje Democracia efectiva y política exterior responsable, en lo referente a los objetivos 5 y 7, estrategias 5.3, 7.1 y 7.2 que a la letra dicen:

Objetivo 5. Promover y garantizar la transparencia, la rendición de cuentas, el acceso a la información y la protección de los datos personales en todos los ámbitos de gobierno.

Estrategia 5.3 Desarrollar el marco normativo que garantice que la información referente a la vida privada y a los datos personales estará protegida.

Objetivo 7. Contribuir a los esfuerzos de la comunidad internacional para ampliar la vigencia de los valores y principios democráticos, las libertades fundamentales y los derechos humanos, así como el desarrollo sustentable.

Estrategia 7.1 Participar activamente en las discusiones e iniciativas en favor de la paz, la cooperación para el desarrollo, los derechos humanos y la seguridad internacionales.

Estrategia 7.2 Incrementar la participación política de México en organismos y foros regionales promoviendo el Desarrollo Humano Sustentable.

3.5 Síntesis Ejecutiva

Como ya se mencionó, el principal propósito de la Red Iberoamericana de Protección de Datos es convertirse en un foro permanente de intercambio de información abierto a todos los países miembros de la comunidad iberoamericana, para promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho de protección de datos personales en un contexto democrático, y lograr que esta regulación sea compatible con otros modelos existentes, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por el derecho ya referido.

Los objetivos específicos de la RIPD:

a) Promover la cooperación interinstitucional y el diálogo entre actores claves para el desarrollo de iniciativas y políticas de protección de datos.
b) Promover políticas, tecnologías y metodologías que permitan garantizar el derecho fundamental a la protección de datos personales.
c) Brindar asistencia técnica y transferencia de conocimientos a los países iberoamericanos que así lo soliciten.

La RIPD se estructura en los siguientes órganos:

I. PRESIDENCIA. La Presidencia de la RIPD es elegida por mayoría simple de entre los miembros presentes en el Encuentro de la RIPD. Corresponde a la Presidencia de la RIPD:

1. Representar a la RIPD en todos aquellos foros nacionales e internacionales en los que se traten aspectos relacionados con la protección de datos.
2. Promover y apoyar en las Cámaras Legislativas nacionales de los países del entorno iberoamericano todas aquellas iniciativas legislativas en proyecto.
3. Promover y representar a la RIPD ante los distintos actores sociales que operan en Iberoamérica y cuya actividad incida en este derecho fundamental.
4. Presidir las reuniones del Comité Ejecutivo.

II. COMITÉ EJECUTIVO. Está constituido por la Presidencia y cuatro Vocalías miembros de la RIPD y tiene las siguientes funciones:

- Asistir a los Encuentros Iberoamericanos de Protección de Datos (EIPDs) y seminarios sectoriales que se celebren durante el ejercicio y decidir sobre los temas relacionados con el funcionamiento y las actividades de la RIPD.
- Aprobar el programa de trabajo del siguiente ejercicio e impulsar todas las actuaciones necesarias para la celebración del próximo EIPD.
- Aprobar la constitución de los Grupos de Trabajo.
- Cooperar activa y periódicamente con la Secretaría en el desarrollo de las funciones que asuman.
- Actuar como revisor editorial de las publicaciones presentadas.

III. SECRETARÍA. La Secretaría de la RIPD se ejerce por la Agencia Española de Protección de Datos, quien asume las tareas de coordinación como órgano técnico y de seguimiento de las actividades de la RIPD. Asumirá las siguientes funciones:

- Mantener una relación continua con el Comité Ejecutivo de la RIPD.

- Establecer contactos con organismos nacionales e internacionales, instituciones afines y cooperantes a fin de gestionar posibles apoyos técnicos y logísticos para el desempeño de las actividades de la RIPD.
- Llevar a cabo junto con los Grupos de Trabajo, el desarrollo de las decisiones y proyectos aprobados en los EIPDs.
- Procurar una comunicación abierta e intercambio de información entre los miembros de la RIPD, atendiendo sus iniciativas y propuestas.
- Coordinar las actividades de los Seminarios y Grupos de Trabajo.
- Instruir las solicitudes de incorporación a la RIPD de nuevos miembros.
- Convocar y colaborar en la organización de los EIPDs.
- Tramitar las invitaciones de expertos y observadores a los EIPDs.

IV. ENCUENTRO IBEROAMERICANO (EIPD). Es la Asamblea General de las Entidades integrantes de la RIPD que se celebrará una vez al año y tendrá el carácter de órgano de la RIPD. El EIPD tendrá naturaleza de foro de discusión directa y de adopción de decisiones y documentos.

Los EIPDs determinarán los seminarios, así como el programa de trabajo durante el año en curso, sin perjuicio de posibles iniciativas que pudieran surgir durante dicho periodo.

El EIPD elegirá por mayoría simple, de entre los miembros presentes, a la Presidencia.

La participación del IFAI dentro de la Red Iberoamericana de Protección de Datos en el periodo comprendido de julio de 2010 a septiembre de 2012, ha tenido el siguiente desarrollo:

Del 21 al 23 de julio de 2010, el IFAI asistió al Seminario Iberoamericano "Nuevas Tecnologías: Seguridad vs Privacidad" realizado en Cartagena de Indias, Colombia.[2] La presencia del Instituto en este seminario fue relevante porque en él los participantes de la Red definieron los temas de la agenda para el VIII Encuentro Iberoamericano de Protección de Datos y determinaron llevarlo a cabo en la Ciudad de México.

De esta manera, el 29 y 30 de septiembre de 2010, México fue la sede del VIII Encuentro Iberoamericano de Protección de Datos. En esta edición los miembros de la Red designaron a México para ocupar la Presidencia para el periodo 2010-2012.[3] Por su parte, como ya está estipulado, a España le corresponde ejercer la Secretaría de esta organización.

Durante el VIII Encuentro se suscribió la "Declaración de México", la cual estableció compromisos para impulsar la promulgación de leyes que reconozcan la protección de datos personales en los gobiernos de la región y avaló la necesidad de contar con estándares regionales e internacionales, con el propósito de ofrecer un modelo de regulación que garantice un alto nivel de protección, pero que al mismo tiempo facilite un intercambio eficiente de datos personales.[4]

[2] Anexo 2
[3] Anexo 3
[4] Anexo 4

El 27 de octubre de 2010, en su calidad de Presidente, el IFAI organizó como primera actividad una reunión del Comité Ejecutivo de la Red, conformado por Costa Rica, Colombia, España, México y Uruguay, el 27 de octubre de 2010, en el marco de la 32 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en la ciudad de Jerusalén, Israel. En dicha reunión se acordó trabajar en la investigación de los siguientes temas de interés: instrumentos de autorregulación; implicaciones económicas del proceso de Adecuación a la Directiva Europea; tratamiento de datos biométricos; transparencia y protección de datos.[5]

En el siguiente año, la Secretaria Técnica de la Red, representada por la Agencia Española de Protección de Datos, y la Presidencia, representada por el IFAI, organizaron los dos seminarios que se contemplan como parte de los acuerdos sostenidos de los Encuentros.

Del 5 al 7 de abril de 2011 se llevó a cabo el primero sobre "Acceso a la información pública y protección de datos; la protección de datos en las cédulas y documentos de identificación de los ciudadanos", en La Antigua, Guatemala. Los objetivos de la actividad se centraron en la presentación, discusión y debate de los temas relacionados con el acceso a la información de tipo público; el acceso y la protección de datos personales y la transparencia en procesos administrativos en los sectores de defensa, seguridad pública, banca, telecomunicaciones, función pública y sector sanidad.[6]

El Seminario dio continuidad a los trabajos de la Red, potenciando así las iniciativas de intercambio de experiencias entre los países iberoamericanos y estableciendo canales abiertos de diálogo y colaboración en materia de protección de datos personales y transparencia, en un marco privilegiado, en la Antigua, donde se gestó el inicio de la Red.

[5] Anexo 5
[6] Anexo 6

En particular, el seminario supuso un salto cualitativo en un doble orden de temas: por una parte, en lo que se refiere al equilibrio entre el derecho de acceso a la información pública y el derecho a la protección de datos personales. Lo anterior fue posible gracias a los análisis conceptuales sobre la interrelación entre ambos derechos y su aplicación práctica en el entorno de las experiencias de los participantes.

Este evento, permitió iniciar una reflexión exhaustiva sobre las implicaciones de los documentos oficiales electrónicos de identificación de los ciudadanos en un ámbito en el que incide un nuevo elemento como son las exigencias de seguridad asociadas a dichos documentos.

El segundo seminario se efectuó del 14 al 16 de junio de 2011, ahora en Cartagena de Indias, Colombia, cuyo tema fue: 'El impacto de las trasferencias internacionales de datos en América Latina. Las políticas preventivas y la autorregulación en la implantación de la normativa de protección de datos'.[7]

En él se abordaron temas como las modalidades de transferencia internacional de datos en los países latinoamericanos, y su incidencia por sectores de actividad, la deslocalización de actividades económicas en América Latina, la experiencia española en políticas preventivas, autorregulación y *enforcement*, experiencias sectoriales de autorregulación, y otros instrumentos preventivos en la aplicación de la normativa de protección de datos.

Asimismo, en el marco del seminario se tuvo oportunidad de sostener una reunión de la Red a puerta cerrada para exponer el avance de los proyectos comprometidos por cada uno de los países del entorno iberoamericano en el VIII Encuentro celebrado en septiembre de 2010 en México.

[7] Anexo 7

Los tres días de actividades permitieron generar un gran debate y una profunda reflexión sobre los temas mencionados, así como continuar con los trabajos de la Red, potenciando las iniciativas de intercambio de experiencias entre los países iberoamericanos y estableciendo canales abiertos de diálogo y colaboración en materia de protección de datos personales.

Posteriormente, en octubre 2011 a México le correspondió organizar y ser sede del IX Encuentro de la RIPD. Este evento se desarrolló en dos sesiones. La primera se realizó en un esquema abierto, en donde se expusieron los siguientes temas:

- Contribución latinoamericana a la modernización del Convenio 108.
- Nuevos avances de la Comisión Federal de Comercio (Federal Trade Commission - FTC) y su implicación en la región.
- Experiencias de los países Iberoamericanos. Casos Perú y Costa Rica.

En esta reunión se contó con la participación del Consejo de Europa quien por primera vez, en el marco de estos eventos presentó “La Contribución de América Latina a la Modernización del Convenio 108”, con la finalidad de recabar las opiniones de la comunidad latinoamericana y tomar en cuenta sus aportaciones en el proceso de reforma del Convenio 108 de la Unión Europea.

La segunda sesión se desarrolló bajo un esquema cerrado, en donde se trataron los siguientes puntos:

- Participación de la RIPD en el desarrollo de una Ley Modelo de la Organización de Estados Americanos (OEA).

- Evolución de la iniciativa de recopilación de Jurisprudencia en materia de protección de datos en los países de la Red.
- Presentación del programa de trabajo 2012.
- Renovación de la Presidencia de la Red y del Comité Ejecutivo (propuesta de candidaturas, votación y toma de posesión).
- Aprobación de la declaración del IX Encuentro.

El IX Encuentro concluyó con la emisión de la resolución 'La Red Iberoamericana de Protección de Datos: un punto de encuentro para afrontar con garantías la globalización', en la que se reconoció que la consecución de un sistema global de protección de datos personales exige promover la confluencia de los sistemas normativos en, al menos, los siguientes aspectos: la aprobación de normativas que ofrezcan un nivel equiparable de protección; la creación de autoridades con competencias adecuadas para garantizar su aplicación; y el impulso de procedimientos de coordinación entre las citadas autoridades que permitan aplicar la normativa sobre protección de datos personales en diversos entornos territoriales y jurídicos.[8]

Durante 2012 el IFAI, en calidad de presidente de la Red, continúa con la promoción y el fortalecimiento de la vigencia de los derechos de acceso a la información y protección de datos en la región, generando y consolidando mecanismos de comunicación entre sus miembros.

En el primer semestre del año, el IFAI en su carácter de presidente de la Red, y en colaboración con la Secretaría Técnica a cargo de la Agencia Española de Protección de Datos (AEPD), organizaron y promovieron los siguientes proyectos:

- El Seminario "Los nuevos retos en materia de protección de datos"

[8] Anexo 8

- El X Encuentro Iberoamericano de Protección de Datos
- El desarrollo jurisprudencial en Iberoamérica en materia de protección de datos
- La revisión del Reglamento para la institucionalización de la Red

Con referencia a la organización del seminario previsto a realizarse en Cartagena, la Agencia Española informó que por cuestiones administrativas y de logística este seminario no se efectuará, para no interferir en tiempo y asistencia con la 34 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad a celebrarse los días 23 y 24 de octubre en Punta del Este, Uruguay.

En cuanto al X Encuentro Iberoamericano su desarrollo se planeó con el formato acostumbrado, una sesión abierta para tratar temas de interés general, y otra sesión cerrada con la finalidad de discutir los temas propios de la Red. En este sentido, para la sesión abierta se contempló un tema sobre las experiencias de algunos países iberoamericanos, los casos de España, Estados Unidos, México y Brasil. En el caso de la sesión cerrada, alguno de los temas relevantes fueron la renovación de la Presidencia y el Comité Ejecutivo, que resultó en la re elección del IFAI como Presidente de la Red para el periodo 2012-2014; asimismo, se discutió la institucionalización de la Red, para lo cual se conformó un grupo de trabajo que se encargará de la revisión del Reglamento y que está conformado por: Brasil, España, México y Portugal. [9]

[9] Anexo 9

Respecto al desarrollo jurisprudencial en Iberoamérica, como ya se destacó, este proyecto surgió como meta del Seminario de Cartagena de 2011, en donde el IFAI se comprometió a realizar un estudio y selección de las sentencias más importantes dictadas por los principales tribunales de cada país o del ámbito regional o internacional con relación a la protección de datos personales, independientemente de que exista o no una ley aprobada sobre la materia. Esto, debido a la heterogeneidad del marco de protección de datos personales en Iberoamérica.

Para ello, el IFAI contrató la asesoría de un experto que a partir de un estudio de derecho comparado analizara los alcances jurídico-interpretativos de la jurisprudencia en materia de protección de datos personales, derecho a la vida privada, intimidad y *habeas data* en Iberoamérica.

El estudio referido contiene los resultados de la investigación, recopilación, análisis y clasificación de los criterios jurisprudenciales relevantes emitidos por los órganos jurisdiccionales iberoamericanos, y el diseño de una plataforma electrónica preliminar para clasificar los fallos jurisprudenciales de los países iberoamericanos.[10]

La consolidación de este proyecto dependerá de la realización de las siguientes actividades: difusión de la plataforma tecnológica entre los miembros de la Red; designación de un responsable por cada Estado miembro que se encargue de publicar y actualizar la información correspondiente; y validación de la información publicada.

[10] Anexo 10

3.6 Acciones realizadas

Con el propósito de que el IFAI organizará el VIII Encuentro Iberoamericano, en la ciudad de México, en septiembre de 2010, el área a cargo del proyecto llevó a cabo las siguientes actividades:

- Determinó los bienes y servicios requeridos para efectuar el VIII Encuentro Iberoamericano de la RIPD.
- Realizó las justificaciones técnicas para su contratación.
- Tramitó la disposición de recursos presupuestales.
- Requirió al área administrativa realizar las acciones de compra conforme la normatividad prevista para ello.

El área financiera autorizó recursos presupuestarios por un importe de $2, 208,236.87-dos millones doscientos ocho mil doscientos treinta y seis pesos 87/100 M.N.- IVA incluido.- para la contratación de servicios relativos a la logística, promoción, hospedaje y alimentación de los asistentes al encuentro; el área administrativa realizó cinco procedimientos de adjudicación directa, en términos de lo establecido en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. Cabe destacar que el importe contratado ascendió a $2,136,108.27 -dos millones siento treinta y seis mil ciento ocho pesos 27/100 M.N.- incluido el IVA, es decir, no se dispuso de $72,128.60 – Setenta y dos mil ciento veintiocho pesos 60/100M.N. de los recursos autorizados, conforme se muestra en el siguiente cuadro:

Relación de Contrataciones, Adquisiciones y/o Gastos

Proyecto Insignia: Red Iberoamericana de Protección de Datos Personales

N° Contrato o pedido	Procedimiento de Contratación, Adquisición y/o Gasto	Empresa u organización	Objeto	Vigencia	Importe en pesos (IVA incluido)			Nivel de cumplimiento
					Presupuesto autorizado	Monto ejercido	Convenios Modificatorios	
063/10	ADJUDICACIÓN DIRECTA	ALGASE, S.A. DE C.V.	SERVICIOS DE HOSPEDAJE, ALIMENTACIÓN Y ESPACIOS FÍSICOS PARA LA REALIZACIÓN DEL VIII ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS	27-09-10 Al 1-10-10	$522,573.80	$522,573.80	NO APLICA	100%
064/10	ADJUDICACIÓN DIRECTA	RESTAURANTES RICLER, S.A. DE C.V.	SERVICIO INTEGRAL PARA EL DESARROLLO DEL ACTO PROTOCOLARIO EN EL MARCO DEL VIII ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS	29-09-10	$45,793.87	$45,793.87	NO APLICA	100%
061/10	ADJUDICACIÓN DIRECTA	ACROM IMPRESORES, S.A. DE C.V.	ELABORACIÓN DE CARTELES Y PROGRAMAS ALUSIVOS AL VIII IBEROAMERICANO DE PROTECCIÓN DE DATOS	24-09-10	$13,189.20	$13,189.20	NO APLICA	100%
059/10	ADJUDICACIÓN DIRECTA	MARIA DEL CARMEN RIVERO VALLS	CONTRATACIÓN DEL SERVICIO DE DISEÑO DEL LOGOTIPO Y DE CARTEL PROMOCIONAL ALUSIVOS AL VIII IBEROAMERICANO DE PROTECCIÓN DE DATOS	09-09-10	$26,680.00	$26,680.00	NO APLICA	100%
C055/10	ADJUDICACIÓN DIRECTA	HECTAREA PRODUCCIONES, S.A. DE C.V.	CONTRATACIÓN DE SERVICIO INTEGRAL DE LOGÍSTICA EN EL MARCO DEL EVENTO "VIII ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS"	25-09-10 Al 7-10-10	$1,600,000	$1,275,826.60	CONVENIO MODIFICATORIO DEL 24 DE SEPTIEMBRE DE 2011, MEDIANTE EL QUE SE AMPLÍA EL MONTO DEL CONTRATO 055/10, ESTABLECIDO EN LA CLÁUSULA TERCERA DEL MISMO, POR UN IMPORTE DE $252,044.80 (DOSCIENTOS CINCUENTA Y DOS MIL CUARENTA Y CUATRO PESOS 80/100 M.N.) CON LO CUAL SE EJERCE UN IMPORTE TOTAL DE $1,527,870.80	100%
					$2,208,236.87	**$1,884,063.47**	**$252,044.80**	

El instituto integró y cuenta con los respectivos expedientes de compra referentes a los pedidos 59/10,61/10,63/10,64/10, y del contrato C055/10.[11]

Es importante señalar que toda la documentación relativa a la Red Iberoamericana de Protección de Datos está disponible en la siguiente dirección: www.redipd.org

3.7 Seguimiento y control

Conforme a lo explicado, la Asamblea General de las Entidades miembros de la RIPD se efectúa una vez al año, en estos encuentros se determinan los seminarios y se diseña el programa de trabajo anual, sin perjuicio de posibles iniciativas que pudieran surgir durante dicho periodo.

Cabe destacar que el Instituto integró al 9° Informe de Labores presentado al H. Congreso de la Unión en 2011, un reporte sobre la participación del IFAI en la Red Iberoamericana de Protección de Datos.

De igual manera, estos resultados se incluyeron en el Informe de Rendición de Cuentas de la Administración Pública Federal 2006-2012.

Este proyecto insignia no ha sido objeto de revisiones por algún ente fiscalizador.

[11] Anexo 12 (Expediente de compra en CD adjunto).

3.8 Resultados y beneficios alcanzados

A ocho años de la constitución de la Red Iberoamericana de Protección de Datos, en la ciudad de Antigua, Guatemala, en 2003, y de haber asumido como principal objetivo el impulso de marcos normativos nacionales que, inspirados en tradiciones jurídicas comunes en el respeto a los derechos fundamentales y en los intereses de sus propios países, garanticen una protección adecuada de los datos personales en todos los países Iberoamericanos, hoy se puede constatar el vertiginoso adelanto del desarrollo de normativas sobre protección de datos en América Latina, movimiento en el que se inscribe nuestro país, con la publicación en 2010, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

Argentina, México, Uruguay, Costa Rica y Perú han legislado en la materia; por su parte Chile, Colombia, Ecuador, Brasil y el Salvador trabajan sobre sus propias iniciativas. Lo que significa que más de 150 millones de ciudadanos latinoamericanos dispongan, junto al tradicional amparo de *habeas data*, de normas que permiten garantizar eficazmente el uso de su información personal y de autoridades especializadas con competencias para tutelar aquellas garantías.

Lo anterior permite afirmar que en los últimos años la región latinoamericana ha ocupado uno de los primeros lugares en el desarrollo de normativas de protección de datos dentro de un mundo globalizado.

México, a través del IFAI, ha participado activamente para contribuir a los esfuerzos de la comunidad internacional, para ampliar la vigencia de los valores y principios democráticos, las libertades fundamentales y los derechos humanos.

3.9 Informe final

A raíz de la creciente importancia que el desarrollo tecnológico ha experimentado en los últimos años, en la región iberoamericana también se ha reflexionado sobre la relevancia del derecho a la protección de los datos y la privacidad, sobre todo como un derecho fundamental de nueva generación que requiere especial consideración de parte de los diferentes gobiernos de la región. En este sentido, desde su creación en 2003, la Red Iberoamericana de Protección de Datos ha representado un foro permanente de intercambio de información abierto a todos los países miembros de la comunidad iberoamericana, con la finalidad de promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho de protección de datos personales en un contexto democrático, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este derecho.

De esta forma, el IFAI desde su inicio ha estado ligado con los trabajos de la Red, sin embargo, fue a partir de 2010 cuando el Instituto comenzó a tener una participación más activa. La publicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en julio de 2010, otorgó a la organización las atribuciones correspondientes para la protección y promoción del derecho, lo que a nivel internacional representó un importante avance para fortalecer la cooperación en la materia con diferentes regiones del mundo, y en especial con Iberoamérica.

En este tenor, en septiembre de 2010 el IFAI organizó el VIII Encuentro Iberoamericano de Protección de Datos, en donde además se le otorgó la Presidencia de la Red por un periodo de dos años; esto significó que a México se le reconociera como un país involucrado en el desarrollo de la protección y promoción del derecho, así como un impulsor en el diálogo entre las diferentes autoridades de protección de datos de la región, y con los expertos y partes privadas involucradas en el tema.

En calidad de Presidente, y en vinculación con la Secretaría Permanente de la Red, representada por la Agencia Española de Protección de Datos, el IFAI se enfocó en promover el diálogo entre los diferentes actores, por lo que tuvo una participación activa en el desarrollo y organización de los dos Seminarios de la Red que se llevaron a cabo durante 2011. Uno de los resultados relevantes de estos Seminarios, fue la propuesta de elaboración de un estudio de jurisprudencia de los países iberoamericanos con la finalidad de impulsar el tema en la región. Asimismo y gracias a la Presidencia de la Red, México logró involucrarse en las discusiones que en materia de protección de datos y privacidad se tienen en el seno de organismos internacionales, como el Consejo de Europa, en donde participó en calidad de observador en las conversaciones sobre la actualización del Convenio 108, al que el país desea adherirse.

Estos trabajos se vieron reforzados con la realización de la 33 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, de la cual México fue sede y el IFAI autoridad anfitriona.[12] Al ser la Conferencia el mayor foro dedicado a la protección de datos y la privacidad a nivel mundial, y que reúne anualmente a las máximas autoridades e instituciones garantes de la protección de datos y la privacidad, además de expertos en la materia de todos los continentes; el Instituto en su papel de Presidente de la Red, y resaltando el hecho de que por primera vez la Conferencia se llevaba a cabo en América Latina, decidió organizar el IX Encuentro Iberoamericano en el marco de este evento. Lo anterior permitió una mayor participación de representantes iberoamericanos y reafirmó el posicionamiento del IFAI en la materia a nivel internacional y en específico con la región iberoamericana.

[12] Anexo 11

Estas experiencias han permitido comprender la importancia que la Red Iberoamericana representa para la región como principal promotor del diálogo, e impulsor de iniciativas y políticas que contribuyan con las que existen en la materia a nivel internacional. A la par de ello, también es importante considerar los retos y áreas de oportunidad que permitan el fortalecimiento y madurez de los proyectos que en la Red se gesten.

Uno de estos desafíos es reformar el Reglamento de la Red para formalizar la participación de los miembros, toda vez que hoy no está constituido como un organismo internacional propiamente, no cuenta con personalidad jurídica, y no está conformado por los representantes de los gobiernos de los países participantes, sino únicamente por quienes pertenecen a un organismo público cuya actuación impacte sobre la protección de datos personales de sus respectivos países. La revisión del Reglamento, formalizada durante el X Encuentro de la Red, permitirá vigorizar los esfuerzos para promover y reforzar la adecuada garantía de este derecho humano a la protección de datos y la privacidad.

VI ENCUENTRO IBEROAMERICANO DE PROTECCION DE DATOS

Con fecha 27 de mayo de 2008 se inauguro el VI Encuentro Iberoamericano de Proteccion de Datos en la ciudad de Cartagena de Indias (Colombia), presidiendo dicho acto el Consul General de Espana en dicha ciudad, **D. Alvaro Ortega Baron,** la Ministra de Comunicaciones de Colombia, **Dna ma del Rosario Guerra** y el Director de la Agencia Espanola de Proteccion de Datos, **D. Artemi Rallo Lombarte.**

Tras una breve pausa comenzaron las exposiciones que llevaban el titulo de **"Seguridad y Proteccion de Datos",** y que fueron impartidas por D. **Hugo Teuffel** III, Director de Privacidad del Departamento de Seguridad Nacional de EEUU, quien destaco la importancia de velar por la privacidad a nivel nacional e internacional, donde la seguridad y privacidad se encuentran estrechamente relacionadas, presentando lo que su departamento ha denominado "practicas justas de informacion", asi como el programa US-Visit, donde detallo a quien correspondia la responsabilidad del tratamiento de la informacion, asi como los objetivos, limitaciones y transparencia de la informacion recogida *y* los principios de confidencialidad, integridad *y* seguridad con que debe tratarse dicha informacion. Tambien menciono los derechos de acceso y rectificacion de los titulares de los datos, finalizando su intervencion aludiendo a la similitud entre Transparencia *y* Confianza, donde detallo los programas, sistemas de notificacion *y* normas existentes en relacion con esta materia, siendo consciente de la diversidad que existe entre cada uno de los paises, pese a reconocer que las practicas justas de informacion suelen ser asumidas por los paises que han legislado en materia de privacidad, destacando especialmente el modelo APEC.

A continuacion, **Dna Isabel Cruz,** Secretaria General de la Comision Nacional de Proteccion de Datos de Portugal realizo una intervencion centrendose especialmente en la seguridad antiterrorista y las diferentes formas graves de delincuencia, destacando el fragil equilibrio que existe entre proteccion de datos y seguridad. La ponencia continuo con una exposicion detallada de la propuesta del PNR europeo de diciembre de 2007 asi como de la Opinion en este sentido del Grupo de Trabajo del articulo 29, finalizando la intervencion con una breve alusion al principio de proporcionalidad en relacion a las replicas Integras de bases de datos frente a accesos funcionales.

Posteriormente **D. Jose Manuel De Frutos,** Administrador Principal de la Direccion General de Justicia, Libertad y Seguridad de la Comision Europea, realizo una exposicion comenzando por la categorizacion del Derecho Fundamental a la proteccion de datos personales y la situacion normativa actual en el ambito de la Union Europea, detallando cada uno de los Tres Pilares. A continuacion el ponente se centro en aspectos particulares como el equilibrio adecuado que ha de lograrse entre los derechos fundamentales y la salvaguardia del interes publico, destacando la falta de armonizacion en determinadas materias penales en las normas comunitarias. Posteriormente menciono una serie de instrumentos comunitarios como el Tratado de Pram asi como la utilizacion de bases de datos comerciales para finalidades policiales, aludiendo a materias concretas como el PNR Europeo (para transporte aereo), el blanqueo de capitales y la utilizacion de datos bancarios (caso SWIFT). FinalizO la intervencion con la importancia del intercambio de informacion en el marco de la cooperacion internacional, asi como destacando la necesidad de establecer normas y principios que respeten el equilibrio entre los derechos fundamentales y este tipo de cooperacion. En ultimo termino se menciono, el Tratado de Lisboa, que en la actualidad se encuentra pendiente de ser aprobado por parte de los paises miembros.

Despues del correspondiente coloquio y de la hora del almuerzo se dio paso al panel

titulado: **"Globalizacion de la Privacidad: hacia unos estandares comunes",** cuyas conferencias correspondieron a **Dna Ma Jose Blanco,** Subdirectora General del Registro General de Proteccion de Datos de la Agencia Espanola de Proteccion de Datos, quien comenzo su exposicion haciendo referencia a los efectos de la globalizacion en materia de proteccion de datos personales dentro del marco de las comunicaciones transfronterizas de flujos de informacion y a la necesidad de lograr el equilibrio entre los intereses empresariales y los derechos individuales. Continuo aludiendo a las principales finalidades *y* actividades que dan lugar a transferencias internacionales de datos *y* los mecanismos *y* garantias de proteccion en el pals de destino *y* las garantias que ha de ofrecer el importador de los datos. A continuacion se citaron las normas que regulan la materia, las novedades introducidas en la legislacion espanola mediante el reciente Reglamento de desarrollo de la LOPD, exponiendo los diferentes supuestos de transferencias internacionales, destacando por su agilidad el reconocimiento de paises con un nivel adecuado de proteccion de datos. Posteriormente la ponente menciono las modalidades de las clausulas contractuales tipo asi como las politicas de proteccion de datos adoptadas en el seno de grupos multinacionales (Binding Corporate Rules). La conferencia finalizo con una breve referencia a datos estadisticos relativos a las transferencias internacionales de datos declaradas en la Autoridad Espanola, con referencia a las autorizaciones del Director de la Agencia a fecha 22 de mayo de 2008, diferenciando los paises del entorno iberoamericano del resto del mundo por el incremento que se ha producido en esta region.

La segunda conferencia correspondiente a este panel fue impartida por **Dna Jacqueline Peschard,** Comisionada del Instituto Federal de Acceso a la Informacion Publica de Mexico, quien abordo la proteccion de datos desde el punto de vista del Foro de Cooperacion Economica Asia-Pacifico (APEC), comenzando con la mencion a los principios generales, sus origenes, los paises que lo constituyen actualmente y continuando con sus objetivos y principios relacionados con la proteccion de datos. Posteriormente se hizo mencion, dentro de APEC, al Grupo Rector de Comercio Electronico y a los subgrupos que lo constituyen, destacando el dedicado a la privacidad, del que se detallaron sus proyectos principales. Finalmente se hizo alusion a los avances mas recientes y compromisos adquiridos en el entorno de APEC, destacando la iniciativa "Explorador de Privacidad de Datos" cuyo principal proposito consiste en facilitar la implementacion del Marco de Privacidad de APEC. En ultimo termino se hizo una comparativa entre el modelo de la Directiva Comunitaria y el modelo APEC, destacando que este ultimo se circunscribe a la actividad comercial de las economias que la integran.

A continuacion, presento su exposicion **D. Juan Ignacio Sanchez,** Subdirector Adjunto de Seguridad y Medio Ambiente de MAPFRE, quien despues de realizar una presentacion de la entidad a la que representaba, continuo realizando una aproximacion historica, analizando las politicas de su entidad para cumplir con la normativa espanola en materia de proteccion de datos, presentando los principales problemas de implantacion con que se encontro dicha empresa y el Plan de Accion que se llevo a cabo para resolver aquellos. Finalizo su intervencion explicando la internacionalizacion de la normativa de proteccion de datos, aludiendo con todo detalle a sus objetivos y proyectos en este sentido y en cada uno de los paises latinoamericanos donde su entidad tiene abiertas diferentes limas de negocio.

Tras una breve pausa D. **Javier Puyol,** Director de la Asesoria Contenciosa y Corporativa del BBVA, introdujo su ponencia desde una perspectiva general para posteriormente centrarse en una serie de criterios de armonizacion y en los denominados estendares comunes en materia de proteccion de datos, haciendo hincapie en la importancia de la seguridad juridica en las reglas del juego economico, y relacionando la proteccion de datos con el gobierno corporativo (principios eticos), protegiendo los datos de

clientes, empleados y accionistas, finalizando su exposicion mencionando las aportaciones que su entidad ha realizado de cara a una homogeneidad legislativa en materia de proteccion de datos. El ponente tambien aludio a la Seguridad y a la Responsabilidad social corporativa.

A continuacion intervino **Dna Gabriela Lopez,** Directora de Privacidad para Latinoamerica de General Electric, quien tras comenzar con una breve exposicion de las lineas de negocio de su entidad, presento los desafios de privacidad para una compania multinacional. Posteriormente destaco la importancia de la proteccion de datos desde un punto de vista normativo, medietico y personal, analizando a continuacion los Estendares de Proteccion de los Datos Personales de los Trabajadores o Reglamentos Corporativos de Carecter Obligatorio (RCO), asi como los principios esenciales y la justificacion de la existencia de un RCO y su proceso de aprobacion. Finalizo su ponencia con el denominado Uso Aceptable de los Recursos de Informacion tanto de su entidad como de terceros que definia concretamente la politica de privacidad de su propia empresa.

La ultima intervencion del dia correspondio a **D. Jose M. De Frutos,** Administrador Principal de la Direccion General de Justicia, Libertad. y Seguridad de la Comision Europea, quien comenzo destacando los efectos de la globalizacion en el ambito de la proteccion de datos, para continuar con una serie de citas correspondientes a textos aprobados en el seno de la OCDE, el Consejo de Europa, la ONU y APEC, recordando el caracter del Derecho Fundamental a la Proteccion de Datos que establece no solo la Constitucion Europea sino ademes la Directiva 95/46/CE. A continuacion realizo una breve alusion a las modalidades posibles de Transferencias Internacionales aun cuando los paises terceros no ofrezcan un nivel adecuado de proteccion, mencionando en ultimo lugar los contratos tipo adoptados por la Comision y las normas corporativas vinculantes (BCRs). Finalizo su exposicion dejando para la reflexion y el debate la posible tension que pudiera apreciarse entre globalizacion y Proteccion de Datos Personales.

El segundo dia del Encuentro, comenzo con las conferencias dedicadas a los **"Nuevos retos en el ambito de la proteccion de datos",** cuya exposicion fue asumida por **D. Cristhian Lizcano,** Director de la Comision de Regulacion de las Telecomunicaciones de Colombia, quien comenzo hablando del Derecho Fundamental de Habeas Data recogido en la Constitucion Politica de Colombia, y sus derechos conexos (informacion, buen nombre, honra e intimidad). La ponencia siguio exponiendo las amenazas y los riesgos frente a los datos personales, tanto desde un punto de vista cientifico y tecnologico asi como las medidas legislativas que han de adoptarse para contrarrestarlas. Posteriormente se destacaron los casos jurisprudenciales mas relevantes, diferenciando el acceso a la informacion de los principios generales de proteccion de datos. A continuacion se expusieron las normas y resoluciones mas importantes aprobadas por el Gobierno colombiano, destacando el ambito de la seguridad e inviolabilidad de las comunicaciones y la estrategia nacional en materia de "ciberseguridad". Se mencionaron los Proyectos de Ley actuales y el Sistema de Seguridad Nacional de la Informacion. Finalizo la intervencion destacando el caracter

constitucional del derecho a la proteccion de datos como garantia fundamental de los ciudadanos y su reconocimiento, dentro del marco de la cooperacion internacional.

En segundo lugar intervino **D. Pedro Less Andrade,** Gerente de Asuntos Gubernamentales y Politicas Publicas de Google para Latinoamerica, quien comenzo destacando la importancia de consensuar el objetivo primordial de su entidad de organizar de forma accesible toda la informacion que reciben y hacerla compatible con la privacidad. A continuacion explico las politicas de privacidad que su empresa intenta transmitir de

manera clara y sencilla a todos los usuarios, informando de los datos que en todo momento se recaban. Posteriormente se explicaron las medidas que su entidad ha ido adoptando en materia de proteccion de datos, como la anonimizacion de logs y la reduccion del tiempo de expiracion de cookies, continuando con los casos de informacion solicitada por parte del Departamento de Justicia de EEUU asi como las resoluciones judiciales dictadas y su implicacion en Europa. El ponente destaco el control que los usuarios tienen de sus datos, pudiendo personalizar su experiencia y su historial Web. Posteriormente se expuso la aplicacion "Street View" *y* sus efectos sobre la seguridad *y* la privacidad, justificando en un momento posterior los anuncios contextuales que utiliza su entidad para financiar los gastos que suponen el servicio de mail gratuito y el funcionamiento de estos. Tambien justifico el porque de conservar determinada informacion, haciendo alusion al caracter de los logs y su funcionalidad, comentando a continuacion las consecuencias negativas de considerar la IP como dato de caracter personal, a pesar de conocer la opinion totalmente contraria de las autoridades de proteccion de datos de la Union Europea en este sentido. En ultimo lugar se hizo mencion a la historia de los estandares globales de privacidad y los requisitos que los mismos han de cumplir para no perder dicho caracter (neutralidad, flexibilidad y actualidad), finalizando con una mencion sobre el desafio de su empresa de innovacion continua dentro del marco de la privacidad.

Posteriormente intervino **Dna ma Luisa Rodriguez Lopez,** Directora de Telecomunicaciones y para la Sociedad de la Informacion de Telefonica, quien inicio su ponencia aludiendo al numero de clientes contabilizados de su empresa, por numero de accesos, la presencia en los diferentes paises de Europa y del resto del mundo, asi como los productos y servicios que en la actualidad presta su entidad. A continuacion menciono la necesaria relacion que ha de existir entre los servicios de comunicaciones electronicas y la proteccion de datos personales, todo ello dentro de lo que denomino la politica corporativa de su empresa, mencionando posteriormente las normas que en la actualidad se encuentran vigentes dicha materia dentro del ambito comunitario, haciendo una especial alusion a las Instrucciones que hasta la fecha ha publicado la Agencia Espanola de Proteccion de Datos, y reconociendo su relevancia a efectos de clarificar su trabajo diario y su forma de actuar en este sentido. En una segunda parte de la exposicion se hablo de la localizacion tanto desde un punto de vista general como especifico, asi como de las diferentes tecnologias utilizadas en GSM (celula de origen, ID de celula mejorada y GPS asistido), continuando con la clasificacion de la localizacion, tanto por tecnologia como por finalidad. Posteriormente menciono los requisitos legales a nivel nacional como europeo asi como las aplicaciones tarifarias basadas en la localizacion, destacando la importancia del consentimiento dentro del contrato especifico asi como la libertad de resolucion del mismo, exceptuando los supuestos recogidos no solo por la Decision del Consejo de 29 de junio de 1991, sino tambien por la Ley General de Telecomunicaciones y los reglamentos de desarrollo aprobados por el Gobierno. En la ultima parte de la conferencia se hizo alusion a los servicios de valor anadido, prestados tanto por el operador como por terceros, basados en la localizacion y sus diferentes modos de acceso. Finalmente hizo una alusion a la Web. 2.0 y el tratamiento de la privacidad.

A continuacion intervino **D. Brendon Lynch,** Director de Privacidad de Microsoft, quien comenzo definiendo el marco de las amenazas cambiantes que en la actualidad estan acechando la privacidad de la informacion en sus diferentes modalidades (phising, spam, pharming, zombies, botnets) dentro del "campo de batalla de Internet", definida esta como descentralizada, anonima y global. Posteriormente se categorizaron los motivos que llevan a provocar tales amenazas asi como el tipo de agentes actuantes y su perfil. A continuacion, y una vez definida su entidad con el logo de "Informatica de confianza", apoyada en los pilares de seguridad, privacidad, fiabilidad y practica de negocios, el ponente detallo el modelo de administracion de privacidad de su empresa, destacando su

caracter general y los estandares de privacidad a todos los niveles, donde un valor encomiable tienen las auditorias independientes que se realizan en dicha entidad, finalizando con la mencion a los principios de privacidad que su entidad publico en Julio de 2007. A continuacion el conferenciante analizo las tecnologias aplicadas a efectos de proteger la privacidad del consumidor y menciono los problemas derivados como consecuencia de la identificacion exacta, fruto de los cuales se han disenado diferentes iniciativas de cara a proteger los posibles danos que pueden sufrir los datos personales. La intervencion finalizo reclamando una vision para una Internet mas segura donde sigue siendo necesaria la adopcion de medidas que protejan la privacidad y haciendo un breve resumen del ciclo vital de la administracion de la informacion, desde su recogida, pasando por su almacenamiento y use hasta su destruccion, asi como de la estructura de la tecnologia para dicha administracion (infraestructura segura, control de identidad y accesos, proteccion de informacion, auditorias e informes), no olvidando la importancia de la privacidad para el avance continuo de un estilo de vida digital en todo el mundo, llevando aparejados beneficios sociales y economicos.

Posteriormente intervino **Dna Ma Pilar Gomez,** Directora de Servicios para la Sociedad de la Informacion de Telefonica, quien inicio su ponencia hablando de las nuevas formas de marketing como instrumento necesario para mantener una gran base de clientes y del marketing o la publicidad viral, que utilizan el efecto "red social", creado por Internet *y* la telefonia mOvil que se caracteriza por su efectividad, credibilidad *y* bajo coste. Posteriormente se citaron las diferentes clases y mecanismos utilizados en esta nueva modalidad de marketing, detallando las caracteristicas que diferencian a cada una de ellas. Tambien se mencionaron los obstaculos con que esta modalidad puede toparse, bien debido a la capacidad de las redes, los formatos de software utilizados, la presencia de antivirus o firewall del usuario o el boicot de las redes sociales por campanas demasiado obvias. La intervencion finalizo haciendo alusion al regimen Juridico de Internet *y* al de su publicidad *y a* los derechos de las personas, tanto desde una perspectiva publica como privada, considerando finalmente la normativa que rige el tratamiento de datos en campanas publicitarias, las comunicaciones comerciales no solicitadas (spam), la obtencion del consentimiento *y* la proteccion de consumidores *y* usuarios, aludiendo en ultima instancia a la Autorregulacion *y* los Codigos de conducta *y a* la politica de gestion del marketing que se sigue en su propia entidad.

Finalizando el panel intervino **Dna Romina Gonzalez Galetto,** Directora General de CoPeerRight Agency Espana, quien tras presentar los origenes y objetivos de su empresa, menciono que su entidad es la primera en Europa en conseguir la autorizacion de la ComisiOn Nacional de Informatica y Libertades (CNIL) para realizar envios de mensajes de prevencion y colectar la direccion IP del primer difusor de una obra. A continuacion detallo los principios (explotar el principio del P2P, disminuir la intrusion y proteger, respetando), objetivos (prevencion, disuasion, interferencia e informacion) y

metodos (redes monitoreadas) que sigue su empresa, asi como las soluciones que aportan en el ambito de las redes sociales P2P, tanto antes como despues de producirse la pirateria, haciendo una breve descripcion funcional de los programas y actividades que su entidad desarrolla. Finalmente se describieron las formas de utilizacion de la IP (anonimizando esta o identificando al difusor *y a* su IP) *y* se analizo el caso concreto de difusion ilegal, concluyendo con la necesidad de lograr el equilibrio justo entre los derechos afectados, siendo un reto para Iberoamerica, dentro de un marco de prevencion y exigencia de las responsabilidades correspondientes.

Tras el debate y la correspondiente pausa del almuerzo, se dio paso a un nuevo panel titulado: **"La Adecuacion Europea",** donde los representantes de **Mexico, Chile,**

Uruguay y Colombia realizaron una exposicion de su situacion normativa actual en materia de proteccion de datos personales, haciendo una extensa exposicion de las iniciativas, proyectos y autoridades e instituciones que en la actualidad se encuentran involucradas en temas directamente relacionados con la Proteccion de Datos Personales, asi como de los principios que rigen cada una de las distintas instituciones que representan, los derechos de las personas, sus mecanismos de reparacion y los bienes juridicos protegidos por su normativa especifica, todo ello con vistas a la posible obtencion de la Declaracion de Adecuacion de la Comision Europea.

El tercer dia del Encuentro comenzo con las exposiciones de los proyectos normativos de **Peru, El Salvador, Costa Rica, Republica Dominicana** en la sesion matinal, coincidentes todos ellos con un reconocimiento del derecho de habeas data, ya sea en una Ley de Acceso a la Informacion Publica, en la norma constitucional correspondiente, en una norma de caracter sectorial, respaldadas por la Code o el Ministerio de Justicia correspondientes, asi como por la Defensoria de los Habitantes y del Consumidor *y* las diferentes Superintendencias de Telecomunicaciones *y* Financieras de ambito nacional.

Despues de una breve pausa continuaron las intervenciones de **Brasil, Ecuador, Honduras, Panama y Guatemala,** cuyas lineas generales vinieron coincidiendo en parte con los ponentes de la sesion de la manana, al existir referencias a la proteccion de datos de una manera muy general en diferentes cuerpos normativos, en cada uno de los paises, y con diferente categoria juridica, si bien hasta la fecha solo puede hablarse de proyectos de ley o tan solo aparecen referencias a la materia en normas sectoriales. Si es cierto que las Leyes de Acceso a la Informacion Publica y Proteccion del Consumidor se han adelantado con caracter general a las normas de proteccion de datos, en buena parte por la ausencia de autoridad nacional independiente y con competencia sancionadora en esta materia.

Tras el descanso propio para comer, se dio paso a una serie de intervenciones que integraban el panel dedicado a las **"Experiencias en proteccion de datos en Estados descentralizados",** inaugurando el mismo **Dna Esther Mitjans i Perello,** Directora de la Agencia Catalana de Proteccion de Datos, quien tras comenzar diferenciando los Estados Centralizados de los Descentralizados, explicando las implicaciones que lleva aparejada la autonomia con caracter general y su reconocimiento constitucional, continuo hablando del nacimiento *y* normativa reguladora de la Agencia Catalana, su estructura, *y* funciones generales (mediacion, supervision, control, formacion, cooperacion), como las correspondientes a cada uno de los Organos que integran dicha institucion, acompanadas por datos estadisticos que reflejaban el trabajo su evolucion durante los ultimos anos. La intervencion finalizo aludiendo a la labor de difusion y divulgacion de dicha agencia.

A continuacion tomo la palabra **Dna Ma Elena Perez-Jaen y D. Agustin Millen,** Comisionados del Instituto de Acceso a la Informacion Publica del Distrito Federal, quienes realizaron dos exposiciones, la primera de ellas centrada en casos significativos de proteccion de datos resueltos por el INFODF de la Ciudad de Mexico (especialmente destacaron los referentes al ambito sanitario y laboral), donde hasta la fecha se ha dado prioridad al derecho de acceso a la informacion publica frente al derecho a la proteccion de datos, pese a la necesidad de aprobar una norma general que regule esta materia, aludiendo en Ultima instancia a la Nueva Ley de Transparencia y Acceso a la Informacion Publica del Distrito Federal, asi como a la constitucion de su Instituto. La segunda intervencion se centro principalmente en los ultimos desarrollos normativos en materia de proteccion de datos, tanto a nivel constitucional como federal, detallando cada uno de los proyectos e iniciativas legislativas tambien en otros estados federales. Finalizo esta

intervencion haciendo una breve alusion a datos estadisticos relativos a las solicitudes de datos personales en los ultimos anos, asi como a los lineamientos de proteccion de datos a nivel federal *y a* la Ley de Transparencia recien aprobada *y* al Proyecto de Ley de Proteccion de datos en el mismo ambito territorial.

Tras una breve pausa comenzaron una serie de intervenciones bajo el titulo: **"Ultimas experiencias en Proteccion de Datos"** cuya primera ponencia correspondio a **D. Thomas Zerdick,** Administrador de la Direccion General de Justicia, Libertad y Seguridad de la Comision Europea, quien comenzando por mencionar los Dictemenes mas recientes aprobados por el Grupo de Trabajo del Articulo 29, continuo detallando cada uno de los pasos necesarios que se han de seguir hasta la obtencion de la Declaracion de Adecuacion por parte de la Comision Europea, poniendo como ejemplo el caso mas reciente de la isla de Jersey.

A continuacion intervino **D. Jesus Rubi,** Adjunto al Director de la Agencia Espanola de Proteccion de Datos, quien comenzo analizando la evolucion de las tareas que ha ido desarrollando la Agencia Espanola, por Areas de trabajo y asuntos, haciendo hincapie en la mayor seguridad juridica que con el tiempo se ha logrado, no solo con la aprobacion del Reglamento de desarrollo de la LOPD, sino tambien con la aportacion de los informes y resoluciones emitidos por la Agencia asi como por las resoluciones de las autoridades judiciales. Finalizo su intervencion declarando los temas mas relevantes que se han ido debatiendo en el Ultimo ano (Buscadores en Internet, redes sociales, P2P, videovigilancia, proteccion de datos y derechos de autor, control en el ambito laboral D).

Finalmente presento su ponencia **D. Eduardo Campos,** Comisario de la Comision Nacional de Proteccion de Datos de Portugal, quien realizo un analisis de las Ultimas iniciativas que su institucion ha presentado en el ambito europeo, especialmente el documento de proteccion de datos de los menores de edad remitido al Grupo de Trabajo del articulo 29, asi como de los temas que en los ultimos meses han sido motivo del mayor numero de consultas y debates suscitados en su pals.

El dia finalizo con una sesion cerrada para los miembros de la Red Iberoamericana de Proteccion de Datos donde se presentaron varios documentos (el Reglamento de la Red, una Declaracion Final del Encuentro asi como una propuesta de actividades para diferentes miembros) cuyo debate y aprobacion quedo pendiente para el dia siguiente.

El ultimo dia del Encuentro, 30 de mayo, comenzo la sesion con el debate de los temas que el dia anterior habian quedado expuestos, a fin de aprobar los documentos mencionados.

Las primeras sugerencias aludieron al contenido del Reglamento, tanto desde el punto de vista sistemetico como en lo relativo a determinados conceptos y terminologia. Se agradecio el esfuerzo notable de la Agencia Espanola de Proteccion de Datos en su labor de asesoramiento de los proyectos normativos de los paises latinoamericanos en orden a obtener la Declaracion de Adecuacion por parte de la Comision Europea.

El fomento de la educacion, la cultura de respeto al Derecho Fundamental a la Proteccion de Datos de caracter personal, los objetivos de la Red y la institucionalizacion de la misma, asi como su trascendencia a foros internacionales, fueron los temas que se debatieron y cuyas sugerencias fueron anotadas para redactar una nueva version de los documentos presentados que recogieran todas las observaciones pertinentes.

En definitiva se alabo por parte de los paises miembros la iniciativa de recoger en un

documento los objetivos de la Red Iberoamericana asi como la creacion de una nueva estructura que la dote de un caracter mas institucional, independientemente de los Grupos de Trabajo especializados que como consecuencia de los diferentes Encuentros Iberoamericanos anuales se celebrasen en un futuro.

A continuacion y por consenso de los asistentes se acordo que la Agencia Espanola de Proteccion de Datos siguiera presidiendo la Red en los dos proximos anos, asi como asumiendo las labores de la Secretaria, aprobendose la eleccion de cuatro nuevas Vocalias que asumirian por el mismo periodo de tiempo: Argentina, Chile, Mexico y Portugal.

Finalmente se aprobo la Declaracion Final del VI Encuentro, anotendose las sugerencias presentadas por los miembros de la Red, asi como el programa de actividades distribuidas entre los diferentes paises propuestos, cuyos compromisos fueron adquiridos de forma voluntaria por cada uno de ellos (se adjunta como **documento anexo).**

Fuera del programa han de destacarse las reuniones bilaterales que mantuvieron los representantes de las delegaciones de Mexico, Chile, Colombia y Uruguay con los Administradores de la Comision Europea a efectos de conocer su situacion normativa actual en materia de proteccion de datos personales de cara a la obtencion de la Declaracion de Adecuacion, *y* en las que estuvieron presentes el Director *y* el Adjunto al Director de la Agencia Espanola de Proteccion de Datos.

En Madrid, a 5 de junio de 2008.

ANEXO
PROGRAMA DE TRABAJO RIPD 2008-2009

a) Organizacion VII Encuentro Iberoamericano de Proteccion de Datos (Mexico).
b) Organizacion de una reunion de trabajo Regional dentro del ambito MERCOSUR (Argentina).
c) Elaboracion de un Boletin de noticias relacionadas con la materia de Proteccion de Datos Personales incluyendo las resoluciones de los Tribunales de Justicia nacionales y los proyectos normativos que se aprueben en cada pals miembro (Mexico).
d) Organizar Seminario de caracter sectorial en Uruguay, durante el ano 2009, aprovechando la creacion del nuevo Centro de Formacion de la Agencia Espanola de Cooperacion Internacional para el Desarrollo en la ciudad de Montevideo. (Uruguay y Espana).
e) Promocionar el Derecho Fundamental a la Proteccion de Datos, durante un mes al ano, coordinando acciones de educacion desde cada una de las instituciones que constituyen la RIPD en cada uno de los paises miembros, presentando la correspondiente evaluacion en el proximo Encuentro Iberoamericano. (Chile).
f) Organizacion de un Seminario de caracter sectorial dentro del ambito Centro America-Caribe. (Mexico y Republica Dominicana).
g) Creacion y coordinacion de un sitio web. de la Red Iberoamericana con acceso general de todos los miembros de la Red. (Espana).

SEMINARIO NUEVAS TECNOLOGÍAS: PRIVACIDAD VS SEGURIDAD
Cartagena de Indias, 21-23 de julio de 2010

MIÉRCOLES 21 DE JULIO DE 2010

09.30 -10.30 INAUGURACIÓN

D. Luis Guillermo Plata. Ministro de Comercio Industria y Turismo.
D. Artemi Rallo. Director Agencia Española de Protección de Datos.

Dña Lidia Blanco. Directora del Centro de Formación

10.30 -10.45 PAUSA-CAFÉ

10.45 -12.30 Seguridad y protección de datos en el transporte aéreo.

Acuerdos "Passenger Name Records", registros de pasajeros, implantación de escáneres corporales y otras medidas de seguridad (pasaportes biométricos, control antecedentes personales,…).

12.30 -13.00 COLOQUIO

13.00 -14.00 COMIDA.

14.00 - 15.00 Seguridad y protección de datos en el sector financiero.

Transferencias financieras. Utilización datos "swift" con fines antiterroristas. Acuerdos internacionales paa el interambio de información personal. Normativa aplicable. Prevención y blanqueo de capitales.

15.00 - 15.30 COLOQUIO

15.30 -15.45 PAUSA-CAFÉ

15.45 -17.00 Seguridad y Privacidad en el marco de las Telecomunicaciones.

Tratamiento de datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas. Brechas de seguridad. La Propiedad intelectual (identificación de usuarios).

17.00-17.30 COLOQUIO

JUEVES 22 DE JULIO DE 2010

09.30-11.00 Protección de datos y Cooperación Policial Judicial.
Política interior y seguridad. La protección de datos personales en el marco de la cooperación policial y judicial en materia penal. Sistemas de información de antecedentes penales. Registro de Penados.

11.00-11.30 COLOQUIO

11.30-11.45 PAUSA-CAFÉ

11.45-13.00 Criminalidad en la Red.
Ciberdelincuencia y Privacidad. Efectos de la "Cloud Computing". Identidad electrónica. Tipificación de delitos: Phising, Bullying, Pharming, Scam, Grooming, Scavenging.

13.00-14.00 COMIDA.

14.00-14.30 COLOQUIO

14.30-15.15 Seguridad y Privacidad en los movimientos migratorios.
Programa de Estocolmo. Acuerdo Schengen, supresión y armonización de controles fronterizos. Comparación de impresiones dactilares. Intercambio de información sobre visados.

15.15-15.30 COLOQUIO

15.30-15.45 PAUSA-CAFÉ

15.45-17.00 Seguridad y Privacidad en los movimientos migratorios (II).
Tratamiento de datos en la legislación nacional (acceso a padrón municipal, consulta selectiva,…).

17.00-17.30 COLOQUIO

VIERNES 23 DE JULIO DE 2010

09.30 -10.30 Tecnología avanzada frente a la limitación de la privacidad.
Reconocimiento mediante videovigilancia + perfil personal.
Tecnologías invasoras/protectoras de la privacidad (esteganografía, criptografía, leyes). Cámaras microscópicas, control remoto. Programa seguimiento personas en 3D. Microchips y RFID (recomendaciones CE).
El papel de las TIC´s en el dilema seguridad vs privacidad.

10.30 -11.00 COLOQUIO

11.00 - 12.00 CONCLUSIONES FINALES.
CLAUSURA.

12.00 - 13.00 COMIDA.

En el marco de las actividades previstas para 2010 por la Red Iberoamericana de Protección de Datos

La RIPD analiza en un seminario el equilibrio entre seguridad y privacidad en el ámbito de las nuevas tecnologías

- **Durante 3 jornadas los asistentes han debatido la compatibilidad entre seguridad y privacidad en sectores como las telecomunicaciones, la banca, el transporte aéreo o la criminalidad en la red, entre otros.**
- **Los expertos destacan que ambos principios no son incompatibles y que el objetivo, ante situaciones de conflicto, es la búsqueda de un equilibrio que garantice los derechos fundamentales.**
- **El director de la AEPD ha destacado la importancia de esta cita anual que permite compartir los avances normativos, lo que debe servir de motivación para los países que aún no han aprobado una ley general en la materia.**

(Madrid, 23 de julio de 2010).- La **Agencia Española de Protección de Datos** (AEPD) ha **organizado junto a la Agencia Española de Cooperación Internacional para el Desarrollo (AECID)** el **Seminario "Nuevas Tecnologías: Seguridad vs. Privacidad",** celebrado en Cartagena de Indias (Colombia), entre el 21 y el 23 de julio, como una de las actividades previstas por la **Red Iberoamericana de Protección de Datos para 2010.**

Durante tres jornadas, representantes de 15 miembros de la Red y del Supervisor Europeo de Protección de Datos (SEPD), así como expertos de la Policía Nacional española, asociaciones civiles y empresas privadas, se han congregado con el objetivo de **analizar el equilibrio entre seguridad y privacidad en el ámbito de las nuevas tecnologías.** En concreto, han debatido cómo se conjugan ambos bienes en sectores como las **telecomunicaciones, las entidades financieras, el transporte aéreo, la criminalidad en la Red, los movimientos migratorios, la cooperación policial y judicial, o el campo de la tecnología avanzada.**

Respecto al equilibrio entre seguridad y privacidad en el marco de las telecomunicaciones, los expertos han retratado una realidad en la que los consumidores son cada vez más conocedores de sus derechos, lo que ha provocado un incremento en el número de prestadores de servicios. En un contexto globalizado en el que la privacidad de los usuarios se ve cada vez más amenazada, se ha resaltado la necesidad de **aprobar medidas de seguridad adecuadas** a la transmisión de los datos, así como la necesidad de identificar los datos que han de ser recopilados y conservados posteriormente.

Asimismo, se han analizado los riesgos para la protección de datos en el **sector financiero,** tales como la captura ilegal de datos o la implantación y uso inadecuado en las nuevas tecnologías. A juicio de los panelistas, los retos se centran, entre otros, en

proteger un número creciente de datos personales, y garantizar la confidencialidad e integridad de la información manejada por terceros y la procesada en otros países.

Otro de los sectores en los que se hace palpable la necesidad de un equilibrio entre seguridad y privacidad es en el **transporte aéreo,** donde tras los atentados del 11-S en Estados Unidos han proliferado los acuerdos de intercambio de información de pasajeros. En este sentido, los asistentes han aludido a la necesidad de impulsar normativas que regulen la recopilación y el almacenamiento de datos personales en América Latina a través de legislaciones concretas. Igualmente, se ha hecho referencia a los escáneres corporales y se han mencionado posibles vías que conjuguen la dignidad humana, los datos personales u otros derechos fundamentales.

Por otra parte, se ha analizado la relación entre **ciberdelincuencia y criminalidad,** donde se ha expuesto una amplia tipificación de los diferentes delitos que pueden cometerse a través de la red, como el *phising, bullying, pharming, scam, grooming o scavenging.* La conjugación entre seguridad y privacidad en el ámbito de los movimientos migratorios ha sido objeto de estudio en un panel, donde se ha hecho referencia a la necesaria congruencia entre la seguridad, libertad y libre tránsito. Según los expertos, **la seguridad personal y ciudadana y el respeto a la privacidad deben combinarse con la garantía de movimientos migratorios ordenados.**

En el campo de la **cooperación policial y judicial,** cuyo objetivo primordial es la investigación de los hechos y la identificación de personas, también se dan situaciones conflictivas, que han sido estudiadas en un panel específico. En él, los expertos han subrayado que el cumplimiento de la ley debe respetar la dignidad y los derechos humanos. Además, han recordado la necesidad de **alcanzar una efectiva protección de los datos personales ante el uso que hacen de ellos las autoridades nacionales.**

Finalmente, se ha analizado la problemática surgida a raíz del **uso de tecnología avanzada,** por ejemplo, los dispositivos de videovigilancia pública. En este sentido, se ha puesto de relieve que la licitud para el uso de una imagen personal por parte de la Policía ha de estar ligada a la investigación del delito, debiendo en caso contrario establecer un uso restringido de los sistemas de videovigilancia.

Una cita anual

El director de la AEPD, Artemi Rallo, ha destacado la importancia de esta cita anual de la **Red Iberoamericana de Protección de Datos,** que **permite compartir los últimos avances normativos** experimentados por países como Perú, Panamá Chile o República Dominicana, junto a los éxitos ya alcanzados de Argentina, Uruguay, Colombia o México, que deben servir de **motivación para los países que aún no han aprobado una ley general en la materia.**

NOTA: Las conclusiones del Seminario "Nuevas Tecnologías: Seguridad vs Privacidad", se encuentran disponibles en la página web de la Red Iberoamericana: (www.redip.org).

SEMINARIO "NUEVAS TECNOLOGÍAS: SEGURIDAD VS PRIVACIDAD"

Durante los días 21 a 23 de julio de 2010, se ha celebrado en el Centro de Formación de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID), en la ciudad de Cartagena de Indias, el "Seminario Nuevas Tecnologías: Seguridad vs. Privacidad". Como una de las actividades aprobadas dentro del marco de la Red Iberoamericana de Protección de Datos para el año 2010, en esta ocasión se han congregado 15 países miembros, representados por 36 instituciones de ámbito nacional y provincial, una representante del Supervisor Europeo de Protección de Datos, del Cuerpo Nacional de Policía de España y a expertos de asociaciones civiles y del sector privado (Google, Yahoo! y Telefónica). En total se presentaron un total de veintiocho intervenciones, conforme al programa diseñado.

El acto inaugural fue presidido por **Dña. Claudia Ramírez,** Viceministra de desarrollo empresarial, del Ministerio de Comercio, Industria y Turismo de Colombia, **D. Artemi Rallo,** Director de la Agencia Española de Protección de Datos (AEPD), **D. Gustavo Valbuena,** Superintendente de Industria y Comercio de Colombia y **Dña. Lidia Blanco,** Directora del Centro de Formación de la AECID en Cartagena de Indias.

La Viceministra Ramírez destacó la importancia de aprobar una Ley General de Protección de Datos en Colombia, informando de la reciente presentación en el Congreso de un proyecto legislativo en materia de protección de datos. Mencionó el volumen de retos que en la actualidad su país debe asumir en esta materia así como la importancia de estas actividades en el marco iberoamericano. El Superintendente Valbuena recalcó los avances normativos experimentados en el último año en Colombia y su efecto económico sobre el incremento competitivo de este país a nivel internacional, garantizando la protección de datos personales junto a la apertura de negocios en el sector de las telecomunicaciones y la implantación de tecnologías de la información. El Director de la AEPD destacó la importancia de esta cita anual que permite compartir los diferentes avances a nivel normativo que han experimentado algunos países de la región como Perú, Panamá, Chile o República Dominicana, junto a los éxitos ya alcanzados de Argentina, Uruguay o México, que deben servir como una motivación para el resto de países que todavía no han aprobado una ley general en la materia. El Director recordó las actividades previstas para el año 2010, así como la convocatoria de la Conferencia Internacional de Autoridades de Protección de Datos del próximo mes de octubre en Jerusalén. Finalmente, hizo referencia al desarrollo de las realidades que se analizarían durante el seminario que junto a ciertas preocupaciones y riesgos, fruto de la globalización, deben conciliarse junto al equilibrio de derechos fundamentales como el derecho a la privacidad.

El primer panel que abrió el seminario abordó el tema de la "**Seguridad y Privacidad en el marco de las Telecomunicaciones**", comenzando el Superintendente de Industria y Comercio de Colombia con un análisis detallado del régimen colombiano de protección de datos personales (inviolabilidad de las comunicaciones, seguridad de los datos, mensajes comerciales o publicitarios y el régimen sancionador) y de las competencias de la Superintendencia en materia de telecomunicaciones. La representante de Telefónica resaltó el incremento del número de prestadores de servicios, frente a consumidores más conocedores de sus derechos. Si bien es cierto que Internet favorece la proliferación de contenidos y facilita menos accesos a la información, también surgen nuevos retos que afectan a la privacidad. Actualmente existe un procedimiento regulado en caso de violación de datos personales que establece una serie de obligaciones explícitas que debe cumplir el prestador de comunicaciones electrónicas junto a los principios generales de consentimiento previo, una amplia legitimación activa, así como la posibilidad de imponer sanciones a dichos prestadores. Se analizaron las novedades incorporadas en

las últimas Directivas Comunitarias en materia de comunicaciones electrónicas y los

principales retos que en materia de privacidad tienen los operadores de telecomunicaciones. Se mencionaron los cuatro principios (libertades) que rigen en materia de protección del derecho a la propiedad intelectual y la neutralidad en la red, recordando que las medidas limitadoras deben ser proporcionadas y sujetas al principio de tutela judicial efectiva, siendo necesaria en todo caso una norma con rango de Ley en lo referente a las medidas garantes del libre ejercicio de la propiedad intelectual.

El representante del IFAI destacó los pilares fundamentales relacionados con la seguridad de la información, como son la proporcionalidad, la integridad y la finalidad, resaltando la necesidad de aprobar medidas de seguridad adecuadas a la transmisión de datos así como la de identificar los datos que han de ser tratados y conservados posteriormente. La intervención de Yahoo! realizó un breve análisis de la evolución de la entidad en materia de privacidad y transparencia, explicando la estructura de su entidad y las medidas de control y protección de la privacidad de los usuarios que han implementado. Resaltaron la transparencia del sitio Web cuando su objetivo es presentar una amplia oferta de servicios, siendo conscientes de las continuas actualizaciones que deben implementar ante al fenómeno de las redes sociales. Finalmente se expusieron distintos proyectos que la entidad ha desarrollado, como Ad Icon, así como la idea de la publicidad personalizada y la experiencia social de compartir información pública en Yahoo!.

La segunda parte de la jornada se dedicó a la ¨**Seguridad y protección de datos en el sector financiero**¨**.** Uruguay expuso la actividad y funcionamiento de las Unidades de Inteligencia Financiera. El ejercicio de los derechos ARCO y la financiación en el marco de las investigaciones sobre el lavado de activos fueron cuestiones que se abordaron y ampliaron con casos jurisprudenciales, dejando abierta la pregunta de quién controla al controlador. También hubo lugar para conocer el marco regulatorio chileno así como el sistema de información financiero y los procesos de comunicación establecidos, identificando la problemática vinculada a la protección de datos personales y a la transparencia del mercado financiero. Posteriormente correspondió el turno al Superintendente Financiero de Colombia, quién analizó la normativa colombiana vigente junto a la estructura, funcionamiento y competencias de la Superintendencia, identificando una serie de riesgos para la protección de datos como: las infidelidades internas respecto al tratamiento de datos, la tercerización de servicios, la captura ilegal de datos o la implantación y uso inadecuado de las nuevas tecnologías. Los retos del sistema financiero se centran en mantener la protección de un número creciente de datos personales, garantizar el acceso de los titulares a la información en los operadores de bancos de datos y fuentes, mantener actualizada la información, garantizar la confidencialidad e integridad de la información manejada por terceros y la procesada en otros países así como administrar los riesgos que conllevan el uso de nuevas tecnologías.

La jornada finalizó con el panel de intervenciones titulado: ¨**Seguridad y protección de datos en el transporte aéreo**¨**.** En esta sección se expusieron los diferentes acuerdos internacionales en materia de intercambio de información de pasajeros así como el tipo de datos transmitidos bajo este tipo de acuerdos. Por parte del IFAI y del Instituto de Transparencia del Estado de Aguas Calientes (México), se analizó el cumplimiento de los principios generales de protección de datos así como el ejercicio de los derechos ARCO a la luz de la implantación de tales acuerdos y sistemas. Una vez más se aludió a la necesidad de impulsar normativas reguladoras del tratamiento de datos personales en América Latina a través de legislaciones concretas. Por parte de la AEPD se analizó esta temática desde la perspectiva de la implantación de escáneres corporales, sus finalidades, el papel de las autoridades, los diferentes sistemas de acceso a la información, así como el tratamiento de datos sensibles que conlleva la implantación de los mismos. Citando la actual Comunicación

de la Comisión al Parlamento Europeo, que establece la necesaria aplicación de los principios de proporcionalidad y finalidad, se mencionaron posibles vías para la protección de la dignidad humana, los datos personales u otros derechos fundamentales. También se analizaron los diferentes sistemas de seguridad, manual o electrónicos a la luz del principio del consentimiento previo al tratamiento de la información personal, finalizando la intervención con una exposición del sistema de control de acceso a zonas restringidas de seguridad que se pretende implantar en los aeropuertos españoles y las repercusiones de dicho sistema, dentro del programa nacional de seguridad, sobre la normativa de protección de datos.

Durante la segunda jornada del seminario se abordó el tema de la **"Criminalidad en la Red",** comenzando por analizar la relación entre la ciberdelincuencia y la privacidad. Posteriormente se expuso el fenómeno de la "Cloud Computing", sus modalidades, aplicaciones, contextos, beneficios (tanto en lo que afecta al acceso a la última tecnología como a la mayor seguridad e innovación) y sus controversias (alta dependencia del proveedor de servicios, integridad, seguridad y privacidad de los datos, aspectos referentes a los derechos de autor de la información, falta de una regulación explícita). A continuación, el representante de Google presentó los principios y herramientas que su entidad facilita a los titulares de los datos para controlar sus datos personales así como los desafíos regulatorios que nos obligan a re-pensar sobre conceptos de privacidad. Dentro del mismo panel pudo conocerse una amplia tipificación de los diferentes delitos que pueden cometerse a través de la red: Phising, Bullying, Pharming, Scam, Grooming, Scavenging. La colaboración ciudadana es considerada una herramienta muy útil para las Fuerzas y Cuerpos de Seguridad que combaten estas categorías delictivas. Además se expuso la normativa uruguaya junto al procedimiento de investigación y la actuación de las autoridades competentes, destacando el rol de AGESIC y su compromiso con la seguridad de la información, partiendo de la protección de los datos personales, como impulsores de la ley vigente y trabajando en la gestión y consolidación del derecho, así como en la salvaguarda de los activos críticos de información del Estado.

La segunda parte de la jornada la protagonizaron los paneles dedicados a la **"Seguridad y Privacidad en los movimientos migratorios",** analizándose por parte de la representante del Supervisor Europeo, el marco legislativo actual, desde la transposición de la Directiva 95/46 CE, el Programa de Estocolmo, los Acuerdos Schengen y el régimen de supresión y armonización de controles fronterizos junto a los nuevos instrumentos electrónicos implantados, los cuáles facilitan la circulación de personas al mismo tiempo que controlan los plazos autorizados de permanencia en una región. Desde dicha institución se incide en la necesaria evaluación de los sistemas existentes a fin de identificar posibles mejoras en su funcionamiento. El IFAI (México) destacó la necesaria ponderación de los derechos fundamentales en el ámbito de la protección de los datos de migrantes y refugiados, donde en ocasiones se mezcla el interés público con el interés estatal, siendo cuestionable en algunos casos la necesidad de publicidad de la información en aras de contribuir al ejercicio de rendición de cuentas por parte de las instituciones públicas en detrimento de la protección de la privacidad. Desde el Instituto Estatal de Acceso a la Información Pública de Oaxaca (México) se analizó el fenómeno migratorio desde un punto de vista histórico, analizando las motivaciones y restricciones que afectan al mismo, destacándose los efectos de las redes sociales en la comunidad de origen de los migrantes en el sentido de facilitar la comunicación y las relaciones sociales. Se insistió en la necesaria promulgación de normas efectivas de protección de datos así como acuerdos entre México y EEUU que garanticen los derechos de los migrantes.

La representante del Tribunal Electoral de Panamá expuso la normativa nacional en materia de acceso a la información pública, planteando la existencia de interrogantes en lo referente a la seguridad y privacidad, siendo consciente de la idiosincrasia y de la diferente problemática que caracteriza a cada país. Desde el

Instituto Coahuilense de Acceso a la Información Pública se hizo una exposición recalcando la necesaria congruencia entre los derechos de seguridad, libertad y libre tránsito, haciendo alusión a la necesaria cooperación a la hora de organizar los movimientos migratorios. La seguridad personal y ciudadana junto al respeto a la privacidad han de conjugarse con la garantía de movimientos migratorios ordenados.

La jornada finalizó con el panel dedicado a la ¨**Protección de Datos y la Cooperación Policial Judicial¨,** interviniendo un representante del órgano Judicial de Panamá, quién compartió con los asistentes la normativa panameña al respecto y destacando entre las finalidades de la cooperación policial judicial el cumplimiento de la ley, el respeto por la dignidad humana y la protección de los derechos humanos. A continuación, en representación de la Corte Superior de Justicia de Lima, se realizó una intervención destacando los principios de verdad procesal y las posibles situaciones conflictivas que pudieran aparecer debido a la preeminencia de determinadas autoridades o de la ineficacia del sistema administrativo judicial vinculado al tratamiento de datos. Se identificaron los agentes protagonistas así como el objeto primordial de la cooperación policial y judicial (investigación de hechos e identificación de personas), las diferentes formas de regulación y los alcances de la cooperación policial y judicial, concluyendo con la necesidad de alcanzar una efectiva protección de los datos ante los diferentes tratamientos realizados por las autoridades nacionales y la falta de una normativa que regule la materia. Por parte de Colombia intervino un juez de Control de Garantías Constitucionales, quién además de mencionar varios textos normativos vigentes, expuso una serie de casos reales de intromisión a la privacidad resueltos por el Consejo de Estado. Finalizando la jornada intervino una representante de la Corte Superior de Justicia de Paraguay, quién aludió a las bases de datos de procesos penales, la legitimación de aceso a la información privada así como las funciones de la Oficina de Estadísticas Penales y la Oficina de Antecedentes Judiciales y sus procedimientos de actuación reglamentados, citando algunas disposiciones específicas sobre el manejo de datos por parte del Poder Judicial y destacando que la interoperabilidad entre el Poder Judicial y la Policía Nacional se circunscribe exclusivamente a la base de datos identificativos de las personas físicas. En último lugar intervino la AEPD, realizando una exposición que partía de la mención de la normativa europea (tratados y directivas actuales) que han resuelto la implantación del Sistema de Información Europeo de Antecedentes Penales (ECRIS), haciendo alusión a la existencia de acuerdos bilaterales y multilaterales y al documento sobre modelos de cláusulas que la Comisión Europea ha redactado a fin de recordar la necesaria observancia de los principios de protección de datos a la hora de firmar este tipo de acuerdos.

La última jornada del seminario se dedicó al panel titulado ¨**Tecnología avanzada frente a la limitación de la privacidad",** iniciando la serie de intervenciones el representante del Registro Nacional de Costa Rica, quién tras realizar un breve balance de los derechos individuales y de la colectividad en Costa Rica, mencionó los efectos sociales y la problemática surgida a raíz del uso de dispositivos tecnológicos de videovigilancia pública, identificando las relaciones existentes entre las diferentes instituciones y el Gobierno así como entre el Poder Ejecutivo y la Sociedad Civil. La licitud del uso de la imagen personal por parte de la Policía ha de estar ligada a la investigación del delito, debiendo en caso contrario establecer el uso restringido de los sistemas de videovigilancia. Por parte del Ministerio de Ciencia y Tecnología de Brasil, se mencionó la normativa específica que regula los sistemas de identificación automática en este país, siendo conscientes de

que la falta de una norma de protección de datos puede llevar en ocasiones a una vulneración de la intimidad en este ámbito. Otro de los temas que se trató fue el registro de acceso a los servicios de Internet y la necesidad del consentimiento previo, libre e informado respecto al tratamiento de datos personales. Finalmente intervino la representante del Supervisor Europeo de Protección de Datos, quién analizó las

recomendaciones del Supervisor en materia del uso de dispositivos RFID (identificadores por radiofrecuencia), mencionando sus diferentes utilidades y los riesgos que pueden entrañar para la privacidad. Terminó su intervención haciendo mención al presente y futuro del diálogo entre el regulador y la industria, considerando los documentos del Grupo de Trabajo del Artículo 29 y de la Agencia Europea de la Sociedad de la Información (ENISA), quiénes se mantienen cautelosos ante el uso de tales dispositivos sin un previo análisis de las medidas de seguridad y de los riesgos para la privacidad que deberían considerarse antes de su implantación global.

El acto de clausura fue presidido por la Directora del Centro de Formación, Lidia Blanco, quién destacó el ejemplo de la Red Iberoamericana como foro de intercambio de experiencias y evolución en los últimos años que permite avanzar en las materias comunes que comparten las instituciones iberoamericanas que forman parte de esta Red. El Adjunto al Director de la AEPD, Jesús Rubí, comenzó destacando la buena salud de que goza la Red Iberoamericana, una Red que no es exclusivamente de la AEPD, sino que abarca a toda la región iberoamericana, la cuál ha experimentado avances legislativos importantes en los últimos años, una presencia institucional cada vez mayor así como la proyección del Derecho Fundamental a la protección de datos en la agenda y en los debates de los distintos países iberoamericanos, algunos de los cuáles ya han iniciado sus procesos de adecuación. Considerando que el Habeas Data ha alcanzado la mayoría de edad, destacó que las leyes de protección de datos han reflejado una protección transversal de los ciudadanos en las más variadas áreas de actividad. Se trata en definitiva de un fenómeno que se retroalimenta, destacando los avances normativos que se producen en cada país y que permiten trasladar el debate a la protección efectiva, ampliándose su actividad a terceros países. Junto a la proyección considerable que ha alcanzado la Red, no hay que olvidar la necesidad de seguir avanzando y consolidar la presencia institucional de cada país miembro, extendiendo los resultados de las actividades celebradas dentro del marco de la Red a los diferentes países y potenciar las herramientas comunes. Finalmente agradeció la colaboración de la AECID y de las instituciones participantes, emplazando a todos los miembros de la Red al próximo Encuentro Iberoamericano que se celebrará en la ciudad de México los días 29 y 30 de septiembre.

En Cartagena de Indias, a 23 de julio de 2010.

VIII ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS

Ciudad de México

29 y 30 de Septiembre de 2010

Presentación.

La Red Iberoamericana de Protección de Datos –en adelante, la Red- se crea mediante la Declaración emitida en el II Encuentro Iberoamericano de Protección de Datos celebrado en La Antigua, Guatemala en 2003, con la anuencia de representantes de los países de Argentina, Brasil, Chile, Costa Rica, El Salvador, España, Guatemala, Nicaragua, Perú, Portugal, Uruguay y México, conscientes del importante papel que juega la protección de datos en el marco de la sociedad de la información y las crecientes relaciones comerciales entre los pueblos iberoamericanos.

Destacan como objetivos de la Red promover la cooperación interinstitucional y el diálogo entre actores claves para el desarrollo de iniciativas y políticas de protección de datos, así como promover políticas, tecnologías y metodologías que permitan garantizar el derecho fundamental a la protección de datos personales.

A fin de cumplir con su cometido, desde su creación la Red ha celebrado anualmente siete Encuentros Iberoamericanos. Estos Encuentros se constituyen como foros de discusión directa y adopción de acuerdos y decisiones de la Asamblea General conformada por los países miembros.

Por tal motivo, México se congratula por ser la sede del **VIII Encuentro Iberoamericano de Protección de Datos** en un momento coyuntural que se caracteriza por un intenso debate sobre la reciente publicación de la Ley Federal de Protección de Datos en Posesión de los Particulares.

Es importante destacar, que en México se han sentado las bases para una regulación integral del derecho a la protección de datos personales, con la aprobación de las reformas a los artículos 16 y 73 constitucionales en el 2009. Estos artículos, reconocen la protección de la información personal como una garantía fundamental, al tiempo de que dotan de facultades al Congreso Federal para expedir una ley secundaria para los particulares - demanda latente desde el 2000-.

Lo anterior, sin menoscabar el notable desarrollo y avances significativos en materia normativa, jurisprudencial y promocional que este derecho fundamental ha tenido en el sector público, a partir de la expedición de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

De esta forma, el VIII Encuentro Iberoamericano pretende constituirse como una plataforma de diálogo y colaboración, a fin de mantener y fortalecer un estrecho y constante intercambio de información,

experiencias y conocimientos entre los países iberoamericanos participantes en esta materia. Asimismo, abrir un espacio de intercambio de experiencias en la región iberoamericana que coadyuven a la protección de los datos personales en el ámbito nacional.

Dentro del marco iberoamericano deben destacarse al mismo tiempo los avances experimentados en la República Oriental del Uruguay con la aprobación de la Ley 18.331 de Protección Datos Personales el 6 de agosto de 2008 y el posterior Decreto de Datos Personales el 31 de agosto de 2009, sobre cuya base el Uruguay ha tomado la iniciativa de solicitar a la Comisión Europea la Decisión como país adecuado conforme a la Directiva 95/46.

Igualmente deben destacarse los avances alcanzados en la República del Perú con la publicación, el 21 de junio de 2010, del Proyecto de Ley de Datos Personales en el portal del Congreso de la República para su correspondiente trámite legislativo, así como en la República de Colombia, con la presentación el 4 de agosto del Proyecto de Ley nº 46 de 2010 "por la que se dictan Disposiciones Generales para la Protección de Datos Personales", firmado por los Ministros del Interior y de Justicia, de Comercio, Industria y Turismo y de Tecnologías de la Información y las Comunicaciones.

Objetivo General.

- Brindar un punto de encuentro para el diálogo, el intercambio y la reflexión en materia de datos personales para los países iberoamericanos, al tiempo de procurar la difusión de la cultura de protección de información de carácter personal.

Objetivos específicos.

- Exponer el grado de avance normativo y jurisprudencial, así como acciones, políticas o programas públicos emprendidos en materia de protección de datos personales de los países iberoamericanos.
- Exponer los avances, retos y perspectivas del derecho a la protección de datos personales en nuestro país.
- Deliberar sobre las ventajas, desventajas y riesgos que entrañan la concepción actual y atribuciones conferidas a órganos garantes de algunos de los países miembros.
- Debatir hasta qué punto son proporcionales las multas económicas e incluso penas corporales -prisión- impuestas a los responsables, por infracciones o delitos cometidos por el uso indebido de información personal.
- Resaltar las bondades y beneficios que representan los esquemas de autorregulación en materias muy específicas que involucran el tratamiento de datos personales para el sector de que se trate, a fin de hacerlo más competitivo a nivel global.

Metodología.

Sesiones matutinas.

- Las sesiones matutinas estarán abiertas al público en general.
- Cada panel tendrá un máximo de 5 expositores, encargados de exponer sus puntos de vista.
- Concluidas sus intervenciones se abrirá la sesión de preguntas.
- El moderador deberá recabar las principales observaciones y hacer una síntesis.

Población objetivo de las sesiones abiertas (agenda matutina).

El VIII Encuentro Iberoamericano está dirigido a integrantes del poder ejecutivo, legislativo y judicial, a servidores públicos, académicos, representantes de la industria, empresas trasnacionales, organizaciones de la sociedad civil y público en general.

Sede

Hotel Royal Pedregal, sito en Periférico Sur No. 4363, Col. Jardines de la Montaña, Deleg. Tlalpan, C.P. 14210, Ciudad de México.

Para mayor información sobre el evento, se podrá consultar el vínculo http://VII Iencuentroiberoamericano.ifai.org.mx

VIII encuentro iberoamericano de protección de datos Ciudad de México

Programa

Miércoles 29 de septiembre de 2010

08:00 – 08:30 hrs.	**Registro**	
8.30 –9:30 hrs.	**Apertura del Encuentro** ~ Artemi Rallo Lombarte, Presidente de la Red Iberoamericana de Protección de Datos y Director de la Agencia Española de Protección de Datos (AGPD), España. ~ Jacqueline Peschard Mariscal, Comisionada Presidenta del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), México. ~ Titulares de dependencias reguladoras: Secretaria de Comunicaciones y Transportes, Secretaria de Economía, Secretaria de Salud y Secretaría de Educación Pública.	
9:30 – 10:00 hrs.	**Conferencia Magistral. "La experiencia canadiense en la materia de protección de datos".** ~ Chantal Bernier, Subcomisionada de la Oficina de Privacidad de Canadá. Presenta: Comisionada Sigrid Arzt Colunga.	
10:00 –10:15 hrs.	**Sesión de preguntas.**	
10:15 –10:30 hrs.	**Receso.**	
10:30 –12:00 hrs.	**Panel 1A. La protección de datos en el sector de las telecomunicaciones.** ~ Felipe Rotondo, Presidente de la Unidad Reguladora y de Control de Datos Personales, Uruguay. ~ Nelson Remolina Angarita, Director del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática, Colombia. ~ Santiago Gutiérrez Fernández, Presidente del Consejo Directivo Nacional de la Cámara Nacional de la Industria Electrónica, de	**Panel 1B. La protección de datos en el sector salud.** ~ Jesús Rubí, Adjunto al Director de la Agencia Española de Protección de Datos, España. ~ Juan Antonio Travieso, Dirección Nacional de Protección de Datos Personales, Ministerio de Justicia, Seguridad y Derechos Humanos, Argentina. ~ María de la Paz Bossio, Directora General de Docencia e Investigación, Ministerio de Salud de Jujuy, Argentina.

	Telecomunicaciones y Tecnologías de la ~Rafael del Villar Alrich, Comisionado, Comisión Federal de Telecomunicaciones, México. Presenta: Comisionado Angel Trinidad Zaldívar.	~ Maki Esther Ortiz Domínguez, Subsecretaría de Integración y Desarrollo de la Secretaría Presenta: Comisionada María Marván Laborde.
12:00 – 12:15 hrs.	**Sesión de preguntas.**	
12:15 – 12:25 hrs.	**Receso.**	
12:25 – 13:55 hrs.	**Panel 2A. Mecanismos sancionadores en caso del tratamiento indebido de datos personales.** ~ Isabel Davara, Académica, Instituto Tecnológico Autónomo de México (ITAM). ~ Emmanuel de Givry, Vicepresidente Delegado, Commission Nationale de l'informatique et des libertés (CNIL), Francia. ~ Artemi Rallo Lombarte, Director de la Agencia Española de Protección de Datos (AGPD). Presenta: Comisionada Presidenta, Jacqueline Peschard Mariscal.	**Panel 2B. Equilibrio entre la protección de datos y el comercio internacional.** ~ Edith Ramírez, Comisionada, Federal Trade Commission, Estados Unidos de Norteamérica. ~ Alfredo Kupfer Dominguez, Socio, Baker & McKenzie, México. ~ Julio César Vega Gómez, Director General de la Asociación Mexicana de Internet (AMIPCI). ~ Claudia Ivette García Romero, Directora General de Comercio Interior y Economía Digital, Subsecretaría de Industria y Comercio de la Secretaría de Economía, México. Presenta: Comisionada María Marván Laborde.
13:55 – 14:10 hrs.	**Sesión de preguntas.**	

Orden del día de la sesión de los miembros de la

Red Iberoamericana de Protección de Datos

Miércoles 29 de septiembre de 2010

(17.00 horas)

- Apertura del Encuentro por Artemi Rallo Lombarte y Jacqueline Peschard Mariscal
- Informe sobre las actividades de la RIPD (revisión de compromisos contraídos en la Declaración de la Antigua).
- Presentación de informes sobre desarrollos normativos y jurisprudenciales de los miembros de la RIPD
- Experiencias en materia de protección de datos personales en el Distrito Federal.
- Renovación de la presidencia de la Red y de los Comités (propuesta de candidaturas y votación).
- Toma de posesión
- Aprobación de la “Declaración de México”.
- Presentación del programa de trabajo 2011.

VIII encuentro iberoamericano de protección de datos Ciudad de México

Jueves 30 de septiembre de 2010

08:30 – 09:30 hrs.	**Registro**	
09:30 – 10:00 hrs.	**Conferencia Magistral. "El derecho a la protección de datos desde el modelo europeo".** ~ José Manuel de Frutos, Dirección General de Justicia, Libertad y Seguridad, Comisión Europea. Presenta: Presidencia de la Red Iberoamericana de Protección de Datos.	
10:00 – 10:10 hrs.	**Sesión de preguntas.**	
10:10 – 11:40 hrs.	**Panel 3A. Distintas experiencias sobre la seguridad de las bases de datos.** ~ Víctor Chapela Barba, Director General de Sm4rt Security Services, México. ~ Ricardo C. Lira Plaza, Socio, Ernst & Young. ~ Eduardo Thill, Subsecretario de la Nación de Tecnologías de Gestión de la Jefatura de Gabinete de Ministros, Argentina. ~ José Manuel Ballester Fernández, Director de Auren, España. Presenta: Comisionada Sigrid Arzt Colunga.	**Panel 3B. La importancia de los mecanismos de autorregulación en el tratamiento de datos personales.** ~ Kim Richardson, Directora Ejecutiva, The Walt Disney Co. ~ Scott Taylor, Director de la Oficina de la Privacidad, The Hewlett-Packard Co. ~ Harry A. Valetk, Director Corporativo de Privacidad, MetLife. ~ Ruth Belcher, Directora de Access Privacy, Canadá. Presenta: Comisionada María Elena Pérez-Jaén Zermeño.
11:40 – 11:50 hrs.	**Sesión de preguntas.**	
11:50 – 12:00 hrs.	**Receso.**	
12:00 – 13:00 hrs.	**Conferencia Magistral. "Casos ilustrativos relevantes sobre el derecho a la privacidad".** ~ Antonio Troncoso Reigada, especialista en materia de protección de datos, España. Presenta: Comisionada María Elena Pérez-Jaén Zermeño.	
13:00 – 13:15 hrs.	**Sesión de preguntas.**	

13:15 – 13:30 hrs.	**Clausura.** • Presidium integrado por las Autoridades de protección de datos de Iberoamérica [España, Uruguay y Colombia]. • Palabras de la Presidencia de la Red Iberoamericana de Protección de Datos.

29 y 30 de Septiembre de 2010 Ciudad de México

Hotel Royal Pedregal -- Periférico Sur No. 4363, Col. Jardines de la Montaña, Delegación Tlalpan.

Organiza el Instituto Federal de Acceso a la Información y Protección de Datos en cola boración con la Red Iberoamericana de Protección de Datos.

Nota de prensa

En el marco del VIII Encuentro Iberoamericano de Protección de Datos, celebrado en Ciudad de México los días 29 y 30 de septiembre

La RIPD suscribe la "Declaración de México" para reforzar las garantías del derecho a la protección de datos en sus países miembros

- **La Declaración constata nuevos riesgos y desafíos para la protección de datos personales.**
- **Los miembros de la RIPD se comprometen a impulsar la promulgación de leyes entre los gobiernos que aún no cuentan con normativa específica en protección de datos y a promover que las autoridades garantes de este derecho posean los recursos necesarios para cumplir con sus obligaciones.**
- **Tras la renovación de cargos, la Comisionada Presidenta del IFAI, Jacqueline Peschard, es la nueva presidenta de la RIPD, y Colombia, Uruguay, Costa Rica y España, los nuevos vocales del Comité Ejecutivo.**

(Madrid, 30 de septiembre de 2010). Los miembros de la Red Iberoamericana de Protección de Datos (RIPD) han suscrito, en el marco del VIII Encuentro Iberoamericano de Protección de Datos celebrado en Ciudad de México los días 29 y 30 de septiembre, la "Declaración de México", que recoge un conjunto de **compromisos orientados a reforzar las garantías de la protección de datos en los países que integran la Red.**

Los miembros de la RIPD constatan cómo el vertiginoso avance de las nuevas tecnologías de la información ha multiplicado los riesgos para la vida privada de las personas, así como la aparición de nuevos desafíos ante servicios como el "cloud computing" -también conocido como la "computación en la nube"- que permiten manejar información fuera de las fronteras nacionales.

También consideran que **el derecho a la protección de los datos personales aún no es valorado ni reconocido en su justa dimensión por algunas autoridades, empresas y por la propia ciudadanía.** La declaración recuerda que existen ámbitos que inciden directamente en la vida privada de las personas, como Internet, que puede generar riesgos para los menores de edad si éstos comparten información sin ningún límite en las redes sociales.

Por ello, se comprometen a **impulsar la promulgación de leyes** entre los gobiernos que aún no cuentan con normativa específica en protección de datos, y a promover que las autoridades encargadas de garantizar este derecho posean la solidez, experiencia, independencia y los **recursos necesarios para cumplir con sus obligaciones.**

Los miembros de la Red también se comprometen a **sensibilizar a la población sobre la importancia de proteger sus datos,** así como a convencer a los gobiernos de la necesidad de adoptar políticas y mecanismos de protección de la identidad. Asimismo, la Declaración insta a **garantizar las medidas de seguridad pública que protejan convenientemente la vida privada de las personas,** de forma que la

recogida y almacenamiento de datos personales se minimice en lo posible y en todo caso, que se haga de forma proporcionada.

Otro de los compromisos suscritos pasa por **impulsar la adopción de estándares regionales e internacionales –como la Resolución de Madrid,** adoptada en el marco de la celebración de la 3 1ª Conferencia Internacional de Autoridades Protección de Datos y Privacidad en 2009- que sirvan como modelos que garanticen un alto nivel de protección y faciliten un eficiente intercambio internacional de datos personales.

Paralelamente, la "Declaración de México" llama a gobiernos, sociedad e industria a **sensibilizar sobre los riesgos que las redes sociales pueden representar para niños y adolescentes;** capacitar a los docentes para que transmitan en un lenguaje claro a los menores los riesgos de proporcionar de manera ilimitada su información personal; concienciar a los padres para que adopten medidas de prevención y alienten el diálogo en familia, y propiciar que los gobiernos establezcan políticas específicas que contemplen la participación de las entidades que tengan injerencia directa o indirecta sobre la educación.

Renovación de cargos

El VIII Encuentro Internacional de Protección de Datos, ha abordado en su sesión vespertina la renovación de los cargos de presidencia y vocales del Comité Ejecutivo de la Red Iberoamericana. El hasta entonces presidente de la RIPD, Artemi Rallo, ha propuesto como nueva presidenta de la Red a Jacqueline Peschard, Comisionada Presidenta del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), quien ha aceptado el cargo.

Por su parte, la recién nombrada presidenta de la RIPD ha presentado una propuesta de renovación de cargos correspondiente a los vocales del Comité Ejecutivo, eligiendo para los mismos a Colombia, Uruguay, Costa Rica y España, que fueron igualmente aceptados.

En el marco del Encuentro, organizado por el IFAI y la RIPD, también se han destacado los avances alcanzados en materia de protección de datos en los marcos normativos de cada uno de los países miembros. En particular, los conseguidos en México, Perú, Colombia y Chile, así como Uruguay, que se encuentra inmerso en pleno proceso de adecuación para obtener la declaración de la Comisión Europea como país con nivel adecuado de protección de datos personales.

"Declaración de México"
VIII Encuentro Iberoamericano de Protección de Datos (2010)

Ciudad de México, 29 y 30 de septiembre de 2010.

Los integrantes de la **Red Iberoamericana de Protección de Datos**, reunidos en la Ciudad de México, nos congratulamos por el desarrollo de los trabajos expuestos en este VIII Encuentro, así como de los avances alcanzados en los diferentes marcos normativos en materia de protección de datos en cada uno de los países miembros.

En particular, deben destacarse los avances alcanzados por la República Oriental del Uruguay con la aprobación de la Ley 18.331 de Protección Datos Personales el 11 de agosto de 2008 y el posterior Decreto de Datos Personales el 31 de agosto de 2009, sobre cuya base, el Uruguay ha tomado la iniciativa de solicitar a la Comisión Europea la Decisión como país adecuado conforme a la Directiva 95/46.

De igual forma, debemos congratularnos por los avances alcanzados en la República del Perú con la publicación, el 21 de junio de 2010, del Proyecto de Ley de Datos Personales en el portal del Congreso de la República para su correspondiente trámite legislativo, así como en la República de Colombia, con la presentación el 4 de agosto del Proyecto de Ley nº 46 de 2010 "por la que se dictan Disposiciones Generales para la Protección de Datos Personales", firmado por los Ministros del Interior y de Justicia, de Comercio, Industria y Turismo y de Tecnologías de la Información y las Comunicaciones.

De manera muy especial, celebramos la reciente entrada en vigor en México, el pasado 6 de julio de 2010, de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, la cual reconoce al Instituto Federal de Acceso a la Información y Protección de Datos, como autoridad garante en la materia, dada su experiencia y solidez en la protección de datos en el ámbito público.

Así, los miembros de la **Red Iberoamericana de Protección de Datos**, CONSIDERANDO que:

- El Encuentro ha abordado y debatido temas de enorme relevancia que indudablemente formarán parte de la agenda internacional, evidenciando una vez más que la Red Iberoamericana se ha convertido en un referente obligado de gobiernos y organizaciones.
- Frente al vertiginoso avance de las tecnologías de la información, los riesgos a los derechos fundamentales y en especial a la vida privada de las personas se han multiplicado.
- Enfrentamos nuevos paradigmas tales como los servicios de manejo de información fuera de las fronteras nacionales conocidos como "la nube" o "Cloud Computing", cuyo desarrollo suscita nuevos desafíos.
- En el ámbito de la seguridad pública, prevalece la existencia de un riesgo real para las personas, ya que bajo dicha premisa se utiliza de manera indebida o errónea su información personal.
- El derecho a la protección de la vida privada de las personas y sus datos aún no es valorado y reconocido en su justa dimensión, por autoridades, empresas y por la propia ciudadanía,
- Internet se ha convertido en un marco de oportunidades, pero también genera riesgos para la integridad física y moral, sobre todo de las niñas, niños y adolescentes, dado que los usuarios comparten información sin límite alguno a través de redes sociales.
- El avance de la genética presenta desafíos para la protección de datos ya que sus descubrimientos pueden tener repercusiones directas en la vida privada de las personas.
- La protección de los datos de las personas por parte de los Estados se dificulta, si se carece del marco legal indispensable y los órganos responsables de su aplicación no cuentan con las condiciones óptimas para el cabal cumplimiento de sus funciones.
- Para lograr su plena vigencia y la legítima competitividad de empresas y naciones, así como la promoción de las inversiones, debe destacarse que el derecho a la protección de la vida privada requiere del trabajo coordinado y del diálogo continuo entre autoridades, sector privado y los propios ciudadanos, y

Por todo lo anterior, SUSCRIBIMOS conjuntamente la **"DECLARACIÓN DE MÉXICO"**, adquiriendo los siguientes compromisos:

1. Impulsar entre los gobiernos de la región que aún no cuentan con desarrollos normativos en la materia, la promulgación de leyes que reconozcan la tutela efectiva de este derecho fundamental.

2. Promover que las autoridades garantes de este derecho cuenten con la solidez, experiencia e independencia suficientes; así como, con los recursos necesarios que les permitan dar cumplimiento cabal a sus obligaciones.

3. Sensibilizar a la población sobre la importancia que reviste la protección efectiva de los datos personales, y convencer a los gobiernos de adoptar políticas y mecanismos en materia de protección de la identidad.

4. Mejorar las prácticas de gestión de datos personales en las organizaciones e instituciones, con el propósito de proteger la identidad de las personas.

5. Garantizar que las medidas relativas a la seguridad pública protejan convenientemente la vida privada de las personas, priorizando los principios de proporción y minimización.

6. Desarrollar la infraestructura operativa y financiera con el propósito de evaluar ex ante la incidencia e impacto de las nuevas tecnologías, sobre la protección de la vida privada.

7. Impulsar la adopción de estándares regionales e internacionales, a fin de ofrecer un modelo de regulación que garantice un alto nivel de protección y facilite un eficiente intercambio internacional de datos personales. En particular, tales como los adoptados a raíz de la Resolución de Madrid, adoptada con motivo de la celebración de la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad en 2009, ofreciendo un modelo de regulación que garantice un alto nivel de protección y por otro facilitar el fluido intercambio internacional de datos personales a efecto de dotar de mayores

garantías a todo tipo de servicios dentro de un mundo globalizado, incluidos los servicios de la nube.

8. Difundir mecanismos con un enfoque holístico, interdisciplinario e integral, a fin de brindar una protección adecuada en el mejor interés de la infancia y la adolescencia. Por ello, gobiernos, sociedad e industria, debemos adquirir compromisos inmediatos, al menos en los siguientes ámbitos:
    a) Sensibilizar sobre los riesgos que las redes sociales en Internet pueden representar para los menores de edad y adolescentes;
    b) Diseñar un enfoque preventivo a través de la educación de los menores, propiciando un compromiso de las autoridades educativas y de la propia industria para capacitar a docentes para transmitir en un lenguaje claro a los menores acerca de los riesgos de proporcionar de manera ilimitada su información personal, al tiempo de brindarles herramientas para hacer un adecuado y productivo uso del Internet y otras telecomunicaciones;
    c) Concientizar a los padres de familia para que adopten en los hogares medidas de prevención y alienten la discusión de estos temas en el seno familiar, y
    d) Propiciar entre los gobiernos, el establecimiento de una política pública ad-hoc que contemple la participación de cada entidad gubernamental que tenga injerencia directa o indirecta sobre la educación.

9. Impulsar marcos normativos que equilibren el desarrollo de la investigación biomédica en beneficio del interés general con garantías adecuadas para la protección de la información personal, incluidas las muestras y datos genéticos.

10. Desarrollar mecanismos de corresponsabilidad con los sectores público, privado y social, que faciliten y promuevan el diseño y desarrollo de programas y acciones que conlleven a la plena vigencia del derecho a la protección de los datos personales.

11. Fomentar que las normativas de protección de datos personales constituyan una herramienta útil y efectiva que facilita las transacciones internacionales y

genera oportunidades de negocio y empleo, con la garantía de defensa de un derecho fundamental.

Si bien es cierto que la tarea a realizar es ardua, los avances aquí recogidos representan, sin duda, un extraordinario aliciente para continuar y ratificar nuestro compromiso a favor de una adecuada protección de los datos de todas las personas. La experiencia demuestra que la consecución de este objetivo se logra con mayor eficacia y legitimidad a través de la participación bajo un enfoque de responsabilidad compartida entre gobiernos, instituciones, empresas y sociedad.

Así lo acordaron los países miembros de la Red Iberoamericana de Protección de Datos, a los 29 días del mes de septiembre de 2010, en la Ciudad de México.

Acta Nº 1. En Jerusalem, el día 27 de octubre de 2010, se reúne el Comité Ejecutivo de la RIPD, estando presente: Jacqueline Peschard, María Elena Pérez-Jaen y Arturo Ríos (México), Jesús Rubí (España), Luis Felipe Torres (Colombia), María José Viega (Uruguay) y Arlin González y Jaime Weisleder (Costa Rica). Se considera el siguiente orden del día:

1. Temas de interés para las reuniones del año 2011, entre los que se mencionan:

a. Instrumentos de autorregulación: se piensa en un enfoque práctico, con planteo de experiencias concretas, en el cual se puede incluir la temática de códigos de conducta, sellos de confianza y normas corporativas vinculantes.

b. Repercusiones económicas de aprobar normativa de protección de datos. Trámite de Adecuación.

c. Tratamiento de Datos Biométricos. El caso de las cédulas de identidad y los documentos de identidad.

d. Transparencia y protección de datos: aspectos prácticos. Los retos de la protección de dos derechos fundamentales a través de una sola autoridad.

2. El borrador de los programas en base a estos temas lo elaborará la Secretaría y los circulará al Comité.

3. Derivado del interés que despierten los temas, se formarán grupos de trabajo a los efectos de elaboran documentos que sean de interés.

4. Se recuerda la importancia de enviar información a Vicente González para la actualización del sitio web y al IFAI para la realización del boletín.

5. Relativo a la propuesta realizada en la última reunión de elaborar un Glosario, se ocupará de la coordinación del tema Costa Rica.

6. México se compromete a presentar un texto sobre los diferentes modelos de autoridades de privacidad.

7. Se encomienda a Uruguay la elaboración del acta de la presente reunión.

Seminario sobre acceso a la información pública y protección de datos; la protección de datos en las cédulas y documentos de identificación de los ciudadanos

La Antigua Guatemala,
Del 05 al 07 de abril de 2011

PROGRAMA

INTRODUCCIÓN

Diversos países latinoamericanos tienen en vigor, desde hace años leyes reguladoras de la transparencia y el acceso a la información pública. En ocasiones estas regulaciones han facilitado el control por parte de los ciudadanos de la actuación de los poderes públicos, mejorando la gobernabilidad.

Estas regulaciones se han incorporado también al sistema legal de países europeos. En el caso español se han fijado las líneas básicas sobre transparencia y acceso a la información. Asimismo, esta materia se ha incorporado a instrumentos internacionales destacando el Convenio Europeo sobre acceso a los documentos públicos, adoptado por el Consejo de Ministros del Consejo de Europa el 27 de noviembre de 2008 y abierto a la firma de los Estados miembros el 18 de junio de 2009.

La transparencia y el derecho de acceso a la información pública están íntimamente relacionados con el derecho a la protección de datos personales ya que la protección de estos puede implicar limitaciones en el acceso a la información.

En particular esta incidencia se manifiesta más intensamente en algunos sectores de la actividad pública como son la defensa y la seguridad, banca, telecomunicaciones, función pública y sanidad entre otros. Los sistemas de garantía de la transparencia y el acceso a la información pública y su conciliación con el derecho a la protección de datos personales son diversos en los países que conforman la red Iberoamericana de protección de datos.

Esta diversidad afecta por un lado a la existencia de una autoridad con competencia en ambas materias o a la creación de dos autoridades diferenciadas, así como a los procedimientos y mecanismos para hacer efectivos ambos derechos.

En los países iberoamericanos se ha puesto de manifiesto una necesidad creciente de articular cédulas y documentos identificativos de los ciudadanos.

El desarrollo tecnológico ha impulsado la creación de documentos oficiales de identidad electrónica que mejoran la identificación de los ciudadanos especialmente a través de medios telemáticos y la seguridad de los documentos. Los documentos de identidad electrónicos incorporan con carácter general datos biométricos de sus titulares asimismo posibilitan la incorporaraciòn de otros datos como pueden ser datos básicos de salud.

Todo ello suscita cuestiones como la legitimación para la creación de estos documentos, la proporcionalidad de los datos que incorporan y la delimitación del acceso a los mismos. De otro lado las medidas de seguridad de estos documentos pueden afectar a las facilidades de su uso por sus titulares.

OBJETIVOS

Los objetivos de la actividad se centrarán en la presentación, discusión y debate de los temas siguientes:

- Acceso a la información de tipo público relacionado con la sanidad y otros temas
- Los sistemas de garantía de la transparencia
- Protección en general de datos personales
- Legitimación para la creación de documentos de identidad

COORDINADORES

D. Jesús Rubí Navarrete
Adjunto al Director
Agencia Española de Protección de Datos. – España

Dña. Lina Zein Gómez de las Heras,
Secretaria Permanente de la Red Iberoamericana
Agencia Española de Protección de Datos. –España

PONENTES

D. Raúl Urrutia Ávila
Presidente
Consejo para la Transparencia. - Chile

Dña. Ximena Oyarzun Aguilar
Encargada de transparencia
Servicio del Registro Civil e Identificación. - Chile

D. Hugo Escalante Sandi
Defensor
Defensoría de los habitantes. - Costa Rica

D. Fernando Arguello Tellez
Magistrado
Corte Suprema de Justicia ante el Tribunal Supremo Electoral. - El Salvador

D. Jorge Adolfo Matheu Fong
Director Ejecutivo
Registro Nacional de Personas RENAP.- Guatemala

Dña. Rosa María de Frade
Presidenta
Comisión de Transparencia del Congreso de la República. – Guatemala

D. Silvio René Gramajo
Director Ejecutivo
Comisión para la Transparencia y Combate a la Corrupción. – Guatemala

D. Arturo Echenique Santos
Comisionado Secretario
Instituto de Acceso a la Información Pública. -Honduras

D. Daniel Regalado Hernández
Asistente Ejecutivo
Instituto de Acceso a la Información Pública. – Honduras

Dña. Lina Ornelas Nuñez
Directora General de Clasificación y Datos Personales
Instituto Federal de Acceso a la Información y Protección de Datos. - México

Dña. Laura de la Borbolla
Directora consultiva
Comisión Nacional Bancario y de Valores. - México

Dña. Sigrid Arzt Colunga
Comisionada
Instituto Federal de Acceso a la Información y Protección de Datos. -México

D. Roberto Corona
Director de Análisis y Proyectos
Instituto Federal de Acceso a la Información y Protección de Datos. -México

Dña. María Elena Pérez-Jaén Zermeño
Comisionada
Instituto Federal de Acceso a la Información y Protección de Datos. - México

D. Víctor Chapela
Director Ejecutivo
Smart Security Services. – México

D. Canek Vázquez Góngora
Presidente del Grupo Plural de Trabajo para revisar el desarrollo de la Cédula de Identidad.
Cámara de Diputados. - México

D. Manuel María Páez Monges
Defensor del Pueblo. – Paraguay

Dña. Berenice Barinas Ubinas
Directora
Oficina de Acceso a la Información Pública en la Procuraduría General de la República. -República Dominicana

Dña. María José Viega
Directora
Dirección de Derechos Ciudadanos de AGESIC. – Uruguay

D. Felipe Rotondo
Presidente
Consejo de la Unidad Reguladora y de Control de Datos Personales - Uruguay

05 martes

08:30	**Traslado Hotel – Centro**
09:00-09:30	**Inscripción y foto individual**
09:30-10-00	**Inauguración**
10:00-10:15	**Pausa café / foto grupal**
10:15-10:45	Derecho de acceso a la Protección de Datos Personales y derecho a la transparencia administrativa. **D. Jesús Rubí Navarrete**
10:45-11:00	Coloquio
11:00-12:45	La incidencia del derecho de acceso a la información pública y la protección de datos personales en los sectores de: defensa y seguridad pública, banca, telecomunicaciones, función pública, sanidad y otros. **Dña. Sigrid Arzt Colunga** **D. Felipe Rotondo** **Dña. Ximena Oyarzun Aguilar** **Dña. Laura de la Borbolla** **Dña. Rosa María de Frade**
12:45-13:00	Coloquio
13:00-14:00	**Almuerzo**
14:00-14:45	Buenas prácticas en el ejercicio del derecho de acceso a la información. **D. Silvio René Gramajo** **D. Manuel María Páez Monges**
14:45-15:00	Coloquio
15:00-15:15	**Pausa café**
15:15-16:45	Experiencias en materia de acceso a la información. **D. Raúl Urrutia Ávila** **Dña. María Elena Pérez-Jaén Zermeño** **D. Fernando Arguello Tellez**
16:45-17:00	Coloquio
17:15	**Traslado Centro - Hotel**

06 miércoles

08:45	Traslado Hotel - Centro
09:00-10:30	Organización y procedimientos para garantizar la transparencia **D. Raúl Urrutia Ávila** **Dña. Lina Ornelas Nuñez** **Dña. Berenice Barinas Ubinas** **Dña. Daniel Regalado Hernández**
10:30-10:45	Pausa café
10:45-11:30	Organización y procedimientos para garantizar la transparencia (Continuación)
11:30-12:00	Coloquio
12:00-13:00	Almuerzo
13:00-14:30	Modelos de autoridades de control en transparencia y protección de datos personales: una autoridad o doble autoridad. **D. Roberto Corona** **D. Arturo Echenique Santos** **Dña. María José Viega**
14:30-14:45	Coloquio
14:45-15:00	Pausa café
15:00-16:00	Presentación del estudio, “Modelos de autoridades de acceso a la información y protección de datos; el equilibrio entre ambos derechos **Dña. Lina Ornelas Nuñez**
16:15	Traslado Centro - Hotel

07 jueves

08:45	Traslado Hotel – Centro
09:00-09:45	Cédulas y documentos de identidad **D. Jesús Rubí Navarrete** **D. Jorge Matheu**
09:45-10:00	Coloquio
10:00-10:15	Pausa café
10:15-11:00	Medidas de seguridad en los documentos de identidad electrónicos **D. Jesús Rubí Navarrete** **D. Víctor Chapela** **D. Hugo Escalante Sandi**
11-:00-11:15	Coloquio
11:45-11:45	El rol de las autoridades. Experiencias compartidas **D. Canek Vázquez Góngora**
11:45-12:00	Coloquio
12:00-12:30	Clausura
12:30-13:30	Almuerzo
13:45	Traslado Centro - Hotel

6ª. Avenida norte entre 3ª. Y 4ª. calle
Antiguo Colegio de la Compañía de Jesús
La Antigua Guatemala
PBX: 7932-3838
FAX: 7832-1280

La Agencia Española de Protección de Datos –AEPD y la AECID han organizado:

Seminario sobre acceso a la información pública y protección de datos; la protección de datos en las cédulas y documentos de identificación de los ciudadanos

- Del 5 al 7 de abril del 2011 en el Centro de Formación de la Cooperación Española en Antigua.
- El acceso y la protección de datos personales y la transparencia en procesos administrativos son el leit motiv del Seminario.

Momento del acto de Inauguración.
Mesa Presidencial (de izq. a drcha.) **Wanda Sigrid Arzt Colunga,** Comisionada del Instituto Federal de Acceso a la Información y Protección de Datos de México; **Jesús Rubí Navarrete,** Adjunto al Director de la Agencia Española de Protección de Datos de España; **Mercedes Flórez,** Directora Centro de Formación de la Cooperación Española en La Antigua Guatemala; **Silvio Gramajo,** Director Ejecutivo de la Comisión para la Transparencia y Combate a la Corrupción de Guatemala.

La Antigua Guatemala 5 de abril de 2011. Hoy se ha inaugurado el ***Seminario sobre acceso a la información pública y protección de datos; la protección de datos en las cédulas y documentos de identificación de los ciudadanos*** en el Centro de Formación de la Cooperación Española en La Antigua Guatemala. El Seminario, que finalizará el jueves 7 de abril, reúne a representantes de universidades, ministerios de justicia, procuradurías y defensorías del pueblo, registros nacionales, ministerios públicos, rentas internas y agencias de Protección de datos y Consejos de Transparencia.

Los objetivos de la actividad se centrarán en la presentación, discusión y debate de los temas relacionados con el acceso a la información de tipo público; el acceso y la protección de datos personales y la transparencia en procesos administrativos en los sectores de defensa, seguridad pública, banca, telecomunicaciones, función pública y sector sanidad.

El nivel de transparencia y la facilidad de acceso a la información pública se consideran hoy, indicadores de los sistemas democráticos. La idea de democracia requiere que lo ciudadanos por sí mismos puedan conocer con mayor amplitud cómo actúan los poderes públicos para controlarlos, detectar los malos funcionamientos y contribuir a mejorar la calidad de la gestión pública, ésta cada vez más extendida en las sociedades democráticas avanzadas.

Por otro lado, los documentos de identidad electrónicos son una herramienta clave para el desarrollo de la sociedad de la información y las relaciones jurídicas y económicas en internet y facilitan el impulso de la administración electrónica con los ciudadanos. Sin embargo, pueden generar riesgos para la privacidad por lo que deben ser compatibles con la protección de datos personales de los ciudadanos.

En los próximos días, los asistentes al Seminario abordarán estos temas con un panel de expertos de diversos países que presentarán las experiencias en la materia.

Esta actividad se enmarca en la Línea del Plan Director de la Gobernabilidad Democrática cuyo objetivo principal es *promover la calidad de la democracia y respeto de los derechos fundamentales* desde una participación real y efectiva de la ciudadanía, el ejercicio de los derechos humanos y las capacidades para promover el desarrollo.

A través de esta actividad se contribuye a la creación de instituciones públicas y estructuras estatales sostenibles que garanticen la gobernabilidad democrática y que lleven a la construcción del estado y a una situación de paz.

En esta actividad está participando la **Red Iberoamericana de Protección de Datos (RIPD**). La misma, surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado en 2003 en este Centro de Formación y que contó con la asistencia de representantes de 14 países iberoamericanos. La RIPD trabaja dando respuesta a la necesidad de fomentar, mantener y fortalecer un estrecho y constante intercambio de información, experiencias y conocimientos entre los Países Iberoamericanos, a través del diálogo y colaboración en materia de protección de datos de carácter personal. Actualmente cuenta con 23 países involucrados. Ver su página web: www.redipd.org .

Centro de Formación de la Cooperación Española

El Centro de Formación de la Cooperación Española en La Antigua Guatemala es una de las cuatro unidades de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID) en el exterior, encargada de coordinar y ejecutar actividades de cooperación en el ámbito específico de la formación. Existen otros tres Centros, en Santa Cruz de la Sierra (Bolivia), Cartagena de Indias (Colombia) y Montevideo (Uruguay). Los cuatro Centros sirven de foro de encuentro de responsables de planificación y ejecución de políticas públicas de Iberoamérica, en todos los ámbitos que son prioritarios del Plan Director de la Cooperación Española 2009-2012. El Centro de Formación de la Cooperación Española de La Antigua Guatemala está ubicado en el antiguo Colegio de la Compañía de Jesús. Anualmente se realizan más de 200 actividades formativas, de carácter nacional e internacional, acogiendo una media de 35 participantes por actividad.

Paralelamente a las actividades formativas, la actividad cultural se ha visto incrementada extensamente; anualmente se organizan conciertos, espectáculos, danza, exposiciones, presentaciones de libros, entre otros. Asimismo, el Centro de Formación cuenta con un Centro de Documentación -Biblioteca, que además de sus fondos especializados en cooperación para el desarrollo, ciencias sociales, historia, literatura y arte, recoge las actividades formativas que aquí se realizan, por lo que constituye un punto de consulta para expertos en desarrollo o en las distintas áreas temáticas en las que se encuentra catalogado.

Para más información:

Belén Marco
Comunicación y Prensa.
Cooperación Española-AECID
La Antigua Guatemala, Guatemala C.A.
6a ave Norte Antiguo Colegio de la Cía de Jesús
TEL: 00(502) 7932-3838
Correo: prensa@aecid-cf.org.gt

EL IMPACTO DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN AMERICA LATINA. LAS POLITICAS PREVENTIVAS Y LA AUTORREGULACION EN LA IMPLANTACION DE LA NORMATIVA DE PROTECCION DE DATOS.

Cartagena de Indias, 14-16 junio 2011

MARTES 14 DE JUNIO DE 2011

09.00 -09.45 INAUGURACIÓN

Dña. Lidia Blanco, Directora del Centro de Formación de la Cooperación Española. (España).

D. Carlos Andrés De Hart Pinto, Viceministro de Desarrollo Empresarial. (Colombia).

D. Jose Miguel de la Calle, Superintendente de Industria y Comercio. (Colombia).

D. Jesús Rubí Navarrete, Adjunto al Director de la Agencia Española de Protección de Datos. (España).

Dña. María Marván Laborde, Comisionada del Instituto Federal de Acceso a la Información y Protección de Datos. (México).

09.45 -10.00 PAUSA-CAFÉ

10.00 -10.30

PONENCIA I: La perspectiva española:

- Modalidades de transferencias. La deslocalización de actividades económicas en América Latina y las cesiones de responsable a encargado del tratamiento.
- Principales sectores relacionados con las transferencias internacionales de datos.

D. Jesús Rubí Navarrete, Adjunto al Director de la Agencia Española de Protección de Datos (España).

10.30 -12.30

PONENCIA II: la incidencia de las modalidades de transferencia internacional de datos en las corporaciones multinacionales:

- **Dña. Natividad Rabazo Auñón**, Gerente de Protección de Datos de Telefonica (España).
- **D. Víctor Manuel Ortega Cárdenas**, Oficial de Protección de Datos de Comunicaciones Nextel de México S.A. (México).
- **D. Javier Puyol Montero**, Director de la Asesoría Jurídica Contenciosa Corporativa del Grupo BBVA (España).
- **D. Jacobo Lázaro Esquenazi Franco**, Director de Relaciones Internacionales con Gobierno para México y Latinoamérica (México).
- **D. Pedro Martín Less Andrade**, Director de Asuntos Gubernamentales y Políticas públicas de Google para América Latina (Argentina).

12.30 -13.00 COLOQUIO.

13.00 -14.00 COMIDA.

14.00 -15.30

PONENCIA III: La perspectiva de los países latinoamericanos por sectores de actividad y países.

- **D. Miguel Ángel Pons Aburto**, Director General de Internet de Telmex (México).
- **D. Francisco Cruz Fuenzalida**, Abogado Asesor de la Corporación de Fomento de la Producción (Chile).
- **D. Santiago Pinzón Galán**, Director Ejecutivo de la Asociación Nacional de Empresarios Industriales (Colombia).

15.30 -15.45 PAUSA-CAFÉ

15.45 -16.45

PONENCIA IV: La modalidades de transferencia internacional de datos y su incidencia en la eficacia para realizarlas:

- Las decisiones de adecuación de la Comisión Europea (decisiones sobre países. El Acuerdo de Puerto Seguro).

D. Rafael García Gozalo, Vocal Asesor - Jefe del área Internacional de la Agencia Española de Protección de Datos (España).

- Las cláusulas contractuales tipo aprobadas por la Comisión Europea.

D. Jesús Rubí Navarrete, Adjunto al Director de la Agencia Española de Protección de Datos (España).

- Las normas corporativas vinculantes (BCR´S).

D. Jacobo Lázaro Esquenazi Franco, Director de Relaciones Internacionales con Gobierno para México y Latinoamérica (México).

- Las CBR's del modelo de APEC.

Harry Armando Valtek, Director Corporativo de MetLife (Estados Unidos de América).

16.45 -17.00 COLOQUIO.

MIÉRCOLES 15 DE JUNIO DE 2011

09.00 -10.00

PONENCIA I: Instrumentos para la aplicación de la normativa de protección de datos. Experiencias en políticas preventivas, autorregulación y enforcement.

Dña. Lina Zein Gómez de las Heras, Consejero Técnico - Secretaría Permanente de la Red Iberoamericana de Protección de Datos de la Agencia Española de Protección de Datos (España).

Dña. Natividad Rabazo Auñón, Gerente de Protección de Datos de Telefonica (España).

Dña. María Marván Laborde, Comisionada del Instituto Federal de Acceso a la Información y Protección de Datos (México).

10.00 -10.15 PAUSA-CAFÉ

10.15 -11.45

PONENCIA II: Instrumentos para la aplicación de la normativa de protección de datos en la perspectiva de los países latinoamericanos:

- **D. Ángel José Trinidad Zaldívar**, Comisionado del Instituto Federal de Acceso a la Información y Protección de Datos (México).

- **Dña. Ema Graciela Romero Silvera**, Abogada de la Dirección de Derechos Ciudadanos de la Agencia para el desarrollo del Gobierno Electrónico y la Sociedad de la Información y el Conocimiento (Uruguay).
- **Dña. Ana María Palacio Valencia**, Asesora del Ministerio de Comercio, Industria y Turismo (Colombia).
- **Dña. Arlene González Castillo**, Directora Jurídica del Registro Nacional (Costa Rica).

11.45-12.30

PONENCIA III: Las exigencias de la autorregulación:

- La vigencia de la legislación sobre la autorregulación.
- Las exigencias para una autorregulación efectiva:

  - La representatividad en los instrumentos de autorregulación.
  - La aportación de valor añadido en los instrumentos de autorregulación.
  - Los sistemas de control interno en la autorregulación.
  - Sistemas arbitrales en la autorregulación.

Dña. Claudia Ivette García Romero, Directora General de Comercio Electrónico, Secretaría de Economía (México).
D. Alejandro del Conde Ugarte, Secretario de Datos del Instituto Federal de Acceso a la Información y Protección de Datos. (México).
D. Felipe Eduardo Rotondo Tornaría, Miembro del Consejo Consultivo de la Unidad Reguladora y de Control de Datos Personales (Uruguay).

12.30 -13.00 COLOQUIO.

13.00 -14.00 COMIDA.

14.00 -15.30 PONENCIA IV: Experiencias sectoriales de autorregulación:

- El modelo de autorregulación en México.
  Dña. Lina Gabriela Ornelas Núñez, Directora General de Autorregulación del Instituto Federal de Acceso a la Información y Protección de Datos. (México).

- El sector sanitario.
  D. Jesús Rubí Navarrete, Adjunto al Director de la Agencia Española de Protección de Datos (España).

- Otras experiencias sectoriales.

D. Rafael Contreras Curiel, Gerente de Sellos de Confianza de la Asociación Mexicana de Internet, A.C. (México).

15.30 -15.45 PAUSA-CAFÉ

15.45 -16.45

PONENCIA V: Otros Instrumentos preventivos en la aplicación de la normativa de protección de datos:

- Las inspecciones sectoriales.

D. Jesús Rubí Navarrete, Adjunto al Director de la Agencia Española de Protección de Datos (España).

- La opciones de la "Privacy by Design" y de las evaluaciones de impacto en la protección de datos (PIA´S).

D. Pedro Less Andrade, Director de Asuntos Gubernamentales y Políticas públicas de Google (Argentina).

16.45 -17.00 COLOQUIO.

JUEVES 16 DE JUNIO DE 2010

09.30 -10.00 CAFÉ

10.00 -12.00 Reunión Cerrada de la Red Iberoamericana de Protección de Datos:

- La Conferencia Internacional.
- La evolución normativa en Latinoamérica.
- Situación y perspectivas de la Red Iberoamericana.

12.00 -13.00 CLAUSURA.

Dña. Lidia Blanco, Directora del Centro de Formación de la Cooperación Española. (España).

D. Jesús Rubí Navarrete, Adjunto al Director de la Agencia Española de Protección de Datos. (España).

D. Ángel José Trinidad Zaldívar, Comisionado del Instituto Federal de Acceso a la Información y Protección de Datos. (México).

13.00 -14.00 COMIDA.

EL IMPACTO DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN AMERICA LATINA. LAS POLITICAS PREVENTIVAS Y LA AUTORREGULACION EN LA IMPLANTACION DE LA NORMATIVA DE PROTECCION DE DATOS.

Durante los días 14 al 16 de junio de 2011, se ha celebrado en el Centro de Formación de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID), en la ciudad de Cartagena de Indias (Colombia), el Seminario "El impacto de las trasferencias internacionales de datos en América Latina. Las políticas preventivas y la autorregulación en la implantación de la normativa de proteccion de datos". En esta ocasión el evento se ha dirigido especialmente a representantes de Instituciones, administraciones y organismos de los países que conforman la Comunidad Iberoamericana, como una de las actividades aprobadas dentro del marco de la Red Iberoamericana de Protección de Datos, reuniendo a nueve países pertenecientes a dicha organización, en su calidad de miembros, asociados u observadores, representados por seis instituciones de ámbito nacional y provincial, al Instituto Federal de Acceso a la Información y Protección de Datos (Presidencia de la RED), a la Agencia Española de Protección de Datos (AEPD, Secretaría Permanente de la RED) y a expertos de asociaciones civiles y empresas multinacionales del sector privado. En total se presentaron un total de veinte intervenciones de países, instituciones (Portugal no estaba) y de asociaciones y empresas del sector privado, conforme al programa diseñado previamente.

El acto inaugural fue presidido por Dña. Lidia Blanco, Directora del Centro de Formación de la Cooperación Española, D. Carlos Andrés de Hart Pinto, Viceministro de Desarrollo Empresarial de Colombia, D. Jesús Rubí Navarrete, Adjunto al Director de la Agencia Española de Protección de Datos, y Dña. María Marván Laborde, Comisionada del Instituto Federal de Acceso a la Información y Protección de Datos.

El primer día del seminario comenzó con la exposición del marco normativo de las transferencias internacionales y de sus excepciones en la LOPD. Se estudiaron las cláusulas contractuales tipo como instrumento de las empresas para solicitar autorizaciones de transferencias internacionales de datos. A continuación se examinó la evolución de los movimientos internacionales de datos inscritos en el Registro General de Protección de Datos y de las autorizaciones otorgadas por el Director de la Agencia, destacando las 378 transferencias declaradas a Argentina a fecha de 31 de marzo de 2011.

En las siguientes ponencias se examinó la incidencia de las modalidades de transferencia internacional de datos en las corporaciones multinacionales. En primer lugar, Telefónica expuso su estructura societaria (Telefónica España, Telefónica Latinoamérica, Telefónica Europa) y expuso su modelo de atención al cliente. Las transferencias internacionales tienen su razón de ser, en este caso, en la necesidad de prestar un servicio

global con gran movilidad laboral, de reducir costes y es en definitiva una apuesta por subcontratar servicios a empresas localizadas en Latinoamérica (Colombia, Perú, Argentina Chile, Paraguay y Guatemala).

Nextel México es una empresa de origen estadounidense, pero tiene gran presencia en países de Latinoamérica: Argentina, Perú, Chile, Brasil y México y ha tenido que adaptarse a la Ley Federal de Protección de Datos Personales en Posesión de Particulares, para lo cual se realizó una auditoria. Actualmente no realiza transferencias internacionales de datos personales de sus suscriptores, sin embargo en el futuro existe un proyecto que en caso de concretarse se concentraría toda la información de sus suscriptores en Estados Unidos de Norteamérica.

El BANCO BILBAO VIZCAYA ARGENTARIA S.A. (BBVA) realiza con carácter general transferencia de datos a países con el mismo nivel de protección, pero aboga por la flexibilidad optando por la posibilidad de transferencia de datos a otros estados que no ofrezcan el mismo nivel de protección cuando el destinatario se comprometa a ese nivel de protección a través de cláusulas contractuales apropiadas. Incluso cuando las transferencias se lleven a cabo en el seno de grupos multinacionales, la garantía consistiría en normas internas de privacidad de carácter vinculante. Defiende el acercamiento del modelo de TID al de las redes sociales y del cloud computing, a través de un modelo con mayor flexibilidad/creatividad y menos formalismo.

Hewlett Packard es una empresa que opera globalmente y ha optado por un modelo de protección de Datos a nivel mundial con el fin de simplificar flujos internacionales y que responda a su responsabilidad social y accountability. Existen varios mecanismos para permitir las TID: contratos modelo, regulaciones, Acuerdo de puerto seguro. Defiende que las empresas también pueden facilitar las TID a través de acuerdos intercompañía, contratos y políticas globales. Las soluciones para el futuro que propone son regulaciones que obliguen a empresas a adoptar políticas globales (como la Resolución de Madrid), y por parte de las empresas que estas adopten normas corporativas vinculantes como Binding Corporate Rules (BCRs) y reglas tras fronterizas de privacidad de APEC (CBPRs).

Posteriormente, en el siguiente panel se examinaron las TDI desde la perspectiva de los países latinoamericanos. CORFO es una agencia gubernamental que apoya el desarrollo económico de Chile, identificó los servicios globales en la industria del offshoring: ITO, BPO, KPO, donde el consumidor del servicio está fuera del país de producción. La protección de datos no es sólo un requisito del negocio de los servicios globales, sino que es un activo agregado del mismo, por lo cual contar con marcos regulatorios adecuados en este ámbito sólo puede generar retornos al país que invierte en ellos, convirtiéndolos en verdaderas plataformas de servicios.

La Asociación Nacional de empresarios de Colombia (ANDI), agrupa a empresas del sector industrial, financiero, de alimentos, comercial, textil y de servicios. ANDI presentó un estudio comparativo de cómo había evolucionado el mundo de los negocios en las dos últimas décadas, estando en la actualidad en la cuarta generación de outsourcing.

La primera jornada finalizó con el examen de las modalidades de transferencia internacional de datos y su incidencia en la eficacia para realizarlas, comenzando por el examen de las Decisiones de Adecuación de la Comisión Europea de conformidad con la Directiva 95/46/CE. Se expusieron los criterios de adecuación del Grupo de Trabajo del artículo 29 de la Directiva y del procedimiento para llevarlo a cabo, aludiendo a un posible cambio en la normativa europea en los mecanismos de transferencias internacionales.

A continuación, se abordó el tema de las cláusulas contractuales tipo para transferencias a encargados de tratamiento en terceros países, tal y como se recoge en la Decisión de la Comisión 2010/87/UE. En la actualidad existe un interés creciente en promover el uso de estas cláusulas a terceros países que no ofrezcan un nivel adecuado de protección, actualizar las cláusulas para abordar nuevos problemas, y finalmente, establecer cláusulas para subencargados del tratamiento.

La ponencia de Hewlett – Pakard se centró en las normas corporativas vinculantes BCR'S, según su modelo global al que se hizo referencia en los párrafos anteriores.

Finalmente, se abordó el modelo de CBPR's según el modelo de APEC en su aplicación por MetLife. En este supuesto, los Reglamentos de datos personales de Estados Unidos requieren que las empresas adopten controles administrativos, técnicos y físicos según el tamaño de la empresa para evitar el riesgo de sobrerregulación. MetLife compartió sus principios corporativos de privacidad y su modelo de protección contra la pérdida de datos.

La segunda jornada se inició con los instrumentos para la aplicación de la normativa de protección de datos. La Agencia Española de Protección de Datos explicó las políticas preventivas llevadas a cabo, tales como las consultas de los ciudadano (presenciales, telefónicas, telemáticas y la divulgación de las guías) las consultas al gabinete jurídico, los seminarios organizados en la Agencia y las reuniones con las empresas. En cuanto al apartado de la autorregulación, se examinó la regulación de los códigos tipo, su tipología y los supuestos prácticos que han supuesto su inscripción en el Registro General de Protección de Datos. En materia de "enforcement", se examinó el volumen de las inspecciones, denuncias, sanciones y tutelas de derechos de conformidad con los datos de la Memoria del año 2010.

La experiencia de Telefónica en políticas preventivas se centra en la grabación de las contrataciones, en la instalación y entrega de los terminales solo a los titulares. En cuanto a los envíos publicitarios se establece como obligación la consulta de las Lista Robinson. Los clientes de Telefónica disponen de una web de protección de datos y el personal está formado en dicha materia. En el ámbito de autorregulación, se analizó el Código Tipo de Protección de Datos de Telefónica de España.

El Instituto Federal de Acceso a la Información y Protección de Datos se propone crear una cultura de protección de datos a través de estudios de impacto, difundir estudios sobre la materia, crear un sistema de gestor de casos para ejercitar los derechos ARCO. En materia de

autorregulación la Ley Federal prevé la adopción de códigos tipo y sellos de confianza. Se explicó el procedimiento de protección de derechos, el procedimiento de conciliación y el procedimiento de imposición de sanciones, incluyendo los tipos penales.

La siguiente ponencia versó sobre los instrumentos para la aplicación de la normativa de protección de datos en la perspectiva de los países latinoamericanos. En México la LFPDPPP reconoce los derechos de tercera generación, en particular la autodeterminación informativa. Uno de los principales desafíos es la elaboración del reglamento.

La experiencia de Uruguay de acuerdo con la Agencia de Gobierno Electrónico y Sociedad de la Información comenzó por una exposición pormenorizada de su normativa y de los pasos que llevaron a su declaración como país adecuado. Se analizaron las bases de datos inscritas, las denuncias, consultas y sanciones impuestas durante el año 2010.

En la actualidad, Colombia cuenta con una legislación penal Ley 1273/2009 de tipificación de conducta por violación de datos personales, y con la Ley 1266/2008 para el sector comercial, financieros, servicios y de datos provenientes de terceros países, siendo el objetivo alcanzar el nivel adecuado por parte de la Unión Europea, para lo cual se ha aprobado una Ley sobre protección de datos personales.

En países como Costa Rica donde al día de hoy no cuentan con una Ley de Protección de Datos y se ha hecho uso de normas dispersas (Constitución Política, Convención América de los Derechos Humanos entre otros) estando fraguándose una regulación sobre la materia. Muchas Instituciones Públicas han tomado conciencia y se han limitado el acceso al uso irrestricto de la información que descansa en sus bases de datos.

El siguiente panel abrió el debate de los instrumentos de autorregulación. La Secretaría de Economía estudió el perfil de dicho país, y expuso la encuesta en materia de protección de Daros realizado a PYMES.

Asimismo, se examinó la autorregulación en la Ley de Protección de Datos Personales en Posesión de los Particulares de México, a través de esquemas de autorregulación que se notifican ante la autoridad sectorial y al IFAI, siendo compatibles con las CBPR's y BCR's.

En Uruguay, la autorregulación cuenta con los siguientes instrumentos: códigos de conducta de práctica profesional, directivas de protección de información personal, códigos de autorregulación, códigos de deontología y códigos tipo, que incluyen normas de seguridad, sellos de calidad, solución arbitral de las controversias y sanciones por incumplimiento.

En la sesión de tarde el debate se centró en las experiencias sectoriales de autorregulación. Comenzó el IFAI exponiendo los lineamientos de protección de datos personales, las verificaciones, las capacitaciones y los impactos a la privacidad.

La Agencia Española de Protección de Datos expuso las responsabilidades en materia de protección de datos en los ensayos clínicos con medicamentos, y los mecanismos de aplicación del código tipo adoptado.

El panel finalizó con la exposición de la Asociación Mexicana de Internet del proyecto de Sellos de Confianza AMIPCI®, como mecanismo de autorregulación en materia de privacidad, enfocado principalmente a la actividad comercial digital.

Las últimas intervenciones se centraron en exponer otros instrumentos preventivos en la aplicación de la normativa de protección de datos personales. En concreto, la Agencia Española de Protección de Datos expuso las Inspecciones Sectoriales llevadas a cabo en los últimos años (en hospitales, Internet, publicidad telefónica, enseñanza, etc.).

La última intervención la realizó un representante de Google quien expuso su política de privacidad de empresa, sobre todo ante los nuevos retos de las redes sociales y cloud computing, para terminar por hacer referencia a las modalidades de TID que realiza dicha empresa a nivel global.

En la última jornada se celebró una reunión cerrada de la RED, en la que se debatieron propuestas de recopilación de jurisprudencia en materia de protección de Datos, de participación en los trabajos sobre protección de datos de la Organización de Estados Americanos (OEA), se presentaron las líneas generales de la Conferencia Internacional que se celebrará en México, y se abordó la celebración del IX Encuentro en dicha Conferencia.

El acto de clausura sirvió como colofón a tres días intensos de debate y reflexión sobre el impacto y regulación de las transferencia internacionales, la deslocalización de actividades económicas en América Latina, las experiencias de los países de la Red en políticas preventivas, autorregulación y enforcement, experiencias sectoriales de autorregulación, y otros instrumentos preventivos en la aplicación de la normativa de protección de datos

El Seminario ha dado continuidad a los trabajos de la Red Iberoamericana de Protección de Datos, potenciando así las iniciativas de intercambio de experiencias entre los países iberoamericanos y estableciendo canales abiertos de diálogo y colaboración en materia de protección de datos personales.

En Cartagena de Indias, a 16 de junio de 2011.

IX ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS

09:30 – 09:45 **INAUGURACIÓN**

- ***Jacqueline Peschard****, Comisionada Presidenta IFAI*
- ***José Luis Rodríguez Álvarez****, Director AEPD.*

SESIÓN ABIERTA

09:45 – 10:45 **CONVENIO 108 Y SU RELACIÓN CON LOS PAÍSES DE LA RED IBEROAMERCIANA**

- ***Jörg Poliakiewicz,*** *Jefe del Departamento de política y desarrollo de los Derechos Humanos, Consejo de Europa*
- ***José Leandro Núñez García,*** Miembro del buró del Comité Consultivo del Convenio 108; asesor en relaciones internacionales, AEPD.

10:45 – 11:00 **COLOQUIO**

11:00 – 11:15 **PAUSA - CAFÉ**

11:15 – 12:15 **NUEVOS AVANCES DE LA COMISIÓN FEDERAL DE COMERCIO (FEDERAL TRADE COMMISSION – FTC) Y SU IMPLICACIÓN EN LA REGIÓN**

- ***Edith Ramírez,*** *Comisionada, Comisión Federal de Comercio (Federal Trade Commision), Estados Unidos de América*

12:15 – 12:30 **COLOQUIO**

12:30 – 13:15 **AVANCES EN EL DESARROLLO DE NUEVAS LEGISLACIONES. LOS CASOS DE COSTA RICA, PERÚ Y COLOMBIA.**

1. La entrada en vigor de la Protección de la Persona frente al tratamiento de sus datos personales, Ley nº 8968 de Costa Rica.
Arlene González Castillo. Costa Rica.

2. La entrada en vigor de la Ley nº 29733 de protección de datos de Perú.
José Álvaro Quiroga. Perú.

3. Actualidad normativa en Latinoamérica: proyecto de leyes de protección de datos.
Luis Felipe Torres Bohórquez. Colombia.

IX ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS

SESIÓN CERRADA

14:30 – 14:45 **REVISIÓN DE AGENDA DE LA SESIÓN**

14:45 – 15:15 **PARTICIPACIÓN DE LA RIPD EN EL DESARROLLO DE UNA LEY MODELO DE LA ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA)**

Presentación de la iniciativa de un proyecto de Ley Modelo de Protección de Datos Personales para el Continente Americano.

- ***David Stewart**, Relator de Privacidad y Protección de Datos Personales de la OEA. Por confirmar.*

15:15 – 15.30 **COLOQUIO**

15:30 – 16:00 **DEFINICIÓN Y AVANCES DE LA INICIATIVA DE RECOPILACIÓN DE JURISPRUDENCIA EN MATERIA DE PROTECCIÓN DE DATOS EN LOS PAÍSES DE LA RIPD (ACUERDOS DE CARTAGENA)**

16:00 – 16:15 **COLOQUIO**

16:15 – 16:30 **PAUSA - CAFÉ**

16:30 - 17:30 **REPORTES DE PAÍS DE LOS MIEMBROS DE LA RED / EXPERIENCIAS DE LOS PAÍSES IBEROAMERICANOS**

1. La entrada en vigor de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.
Representante Del IFAI. México.

2. Experiencias en el desarrollo de la protección de datos.
Representante de la Agencia Española de Protección de Datos. España.

17:30 – 17:45 **COLOQUIO**

17:45 – 18:00 **PAUSA CAFÉ**

18:00 – 18:15 **ASUNTOS GENERALES / PRESENTACIÓN DEL PROGRAMA DE TRABAJO 2012**

18:15 – 18:30 **APROBACIÓN DE LA DECLARACIÓN DEL IX ENCUENTRO**

18:30 – 18:45 **CLAUSURA**

- ***Jacqueline Peschard**, Comisionada Presidenta IFAI*
- ***José Luis Rodríguez Álvarez**, Director AEPD.*

RESOLUCIONES DEL NOVENO ENCUENTRO DE LA RED IBEROAMERICANA DE PROTECCION DE DATOS

LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS: UN PUNTO DE ENCUENTRO PARA AFRONTAR CON GARANTÍAS LA GLOBALIZACIÓN

La Red Iberoamericana de Protección de Datos, constituida en Antigua Guatemala en el año 2003, asumió como principal objetivo el impulso de marcos normativos nacionales que, inspirados en tradiciones jurídicas comunes en el respeto a los derechos fundamentales y en los intereses de sus respectivos países, garantizaran una protección adecuada de los datos personales en todos los países Iberoamericanos.

Transcurridos ocho años desde la Declaración de La Antigua, el desarrollo de normativas sobre protección de datos en Latinoamérica ha experimentado una intensa evolución.

Además de la iniciativa argentina, anterior a la constitución de la Red, desde 2003 se han promulgado leyes de protección de datos personales en Uruguay, México, Costa Rica, Perú y se está revisando en Chile. Y existen iniciativas en tramitación en países como Colombia, Ecuador, Brasil y El Salvador.

Más de 150 millones de ciudadanos latinoamericanos disponen, junto al tradicional amparo de habeas data, de normas que permiten garantizar eficazmente el uso de su información personal y de autoridades especializadas con competencias para tutelar aquellas garantías.

Lo que permite afirmar que en los últimos años el área de la región latinoamericana ha ocupado uno de los primeros lugares en el desarrollo de normativas de protección de datos dentro de un mundo globalizado.

Junto a ello, la Red Iberoamericana de Protección de Datos ha iniciado un proceso para su institucionalización, acordando la asunción de su Presidencia por Instituciones del prestigio del Instituto Federal de Acceso a la Información y Protección de Datos de México (IFAI).

El reconocimiento internacional de las Autoridades latinoamericanas de protección de datos se ha refrendado con la designación del IFAI como organizador de la 33ª Conferencia Internacional de Comisionados de Protección de datos y de la Privacidad, que se celebrara del 1 al 3 noviembre en México, D.F.

La Red Iberoamericana de Protección de Datos es consciente y reitera su compromiso respecto a que la adopción de estándares regionales e internacionales que garanticen un alto nivel de protección de los datos

personales, facilitará un eficiente desarrollo de los flujos internacionales de datos que redundarán en el desarrollo de actividades económicas con garantías para los ciudadanos, con independencia del país de su residencia.

En este sentido, reafirma que los estándares internacionales adoptados en la Resolución de Madrid ofrecen un modelo de regulación flexible y adaptable a una diversidad de culturas jurídicas, como se ha acreditado en la aprobación de las normas de protección de datos en países latinoamericanos.

La Red Iberoamericana de Protección de datos manifiesta su carácter abierto y su voluntad de servir de punto de encuentro con los países próximos a su entorno y con las corporaciones multinacionales que operan globalmente.

Parte de sus miembros lo son también de otros ámbitos regionales, tales como el Foro de Cooperación Económica Asia Pacífico (APEC), y mantienen relaciones próximas con los Estados Unidos de América, Canadá y la Unión Europea.

El IX Encuentro de la Red ha permitido constatar el interés mutuo en la protección de la privacidad, con la participación del Consejo de Europa y de la Comisión Federal de Comercio de los Estados Unidos (FTC), que se une a la relación fraterna mantenida con los países integrados en la Asociación Francófona de Autoridades de Protección de Datos Personales.

La consecución de un sistema global de protección de datos personales exige promover la confluencia de los sistemas normativos en, al menos, los siguientes aspectos:

- La aprobación de normativas que ofrezcan un nivel equiparable de protección.
- La creación de autoridades con competencias adecuadas para garantizar su aplicación.
- El impulso de procedimientos de coordinación entre las citadas autoridades que permitan aplicar la normativa sobre protección de datos personales en diversos entornos territoriales y jurídicos.

Sobre estas premisas, los integrantes de la Red Iberoamericana de Protección de Datos, reunidos en la Ciudad de México, asumimos los siguientes compromisos:

- La voluntad de servir de punto de encuentro para las iniciativas que desde los más diversos ámbitos regionales promuevan la protección de datos personales en un entorno global.

- Colaborar activamente, partiendo de las experiencias de los distintos países, en la elaboración de una ley modelo sobre la protección de datos en la Organización de Estados Americanos.

- Intensificar la promoción de la normativa de protección de datos personales en el ámbito Iberoamericano.

-. Fomentar la participación de Autoridades homólogas, que sin ser parte de la Red pueden contribuir con su experiencia, tal es el caso de Canadá y Estados Unidos de América en las actividades de la Red.

- Poner en común los desarrollos jurisprudenciales de la Región, a través de herramientas de consulta acerca de los criterios más avanzados en materia de protección de datos; privacidad y habeas data.

- Dar a conocer las propuestas de otras iniciativas regionales.

- Difundir entre los miembros de la Red Iberoamericana de Protección de Datos las experiencias de APEC sobre la materia.

-Dar a conocer las propuestas de modernización del convenio 108, del Consejo de Europa.

- Coordinar el impulso a la protección de la privacidad con la Asociación Francófona de Autoridades de Protección de Datos Personales, a través del intercambio de experiencias y conocimiento.

- Impulsar la participación de corporaciones multinacionales en el análisis y evaluación de la protección de datos personales en un mundo globalizado y su incidencia en América Latina, así como promover modelos de autorregulación homologables.

- Promover la homologación de las Autoridades de Protección de datos atendiendo a las especificidades de los diversos sistemas jurídicos.

- Desarrollar procedimientos transfronterizos de cooperación que contribuyan a garantizar los derechos a los ciudadanos.

- Facilitar el intercambio de tecnologías entre Autoridades con el fin de minimizar costes y homogeneizar sistemas de información y cumplimiento.

- Promover intercambios de información entre las Autoridades de Protección de Datos miembros de la Red Iberoamericana para establecer criterios armonizados en la aplicación de las leyes nacionales.

- Acentuar las acciones formativas entre los miembros de la Red Iberoamericana de Protección de datos.

REGLAMENTO RED IBEROAMERICANA DE PROTECCIÓN DE DATOS (RIPD)

La Red Iberoamericana de Protección de Datos (RIPD), surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, con la asistencia de representantes de 14 países iberoamericanos.

LA RIPD se constituye como una respuesta a la necesidad de fomentar, mantener y fortalecer un estrecho y constante intercambio de información, experiencias y conocimientos entre los Países Iberoamericanos, a través del diálogo y colaboración en materia de protección de datos de carácter personal. La RIPD se encuentra abierta a todos los países iberoamericanos que deseen promover y ejecutar iniciativas y proyectos relacionados con esta materia.

La RIPD pretende crear un foro integrador que permita involucrar a diversos actores sociales, tanto del sector público como privado.

Esta iniciativa contó desde sus inicios con un apoyo político reflejado en la Declaración Final de la XIII Cumbre de Jefes de Estado y de Gobierno de los países iberoamericanos celebrada en Santa Cruz de la Sierra, Bolivia, 14 y 15 de noviembre de 2003, conscientes del carácter de la protección de datos personales como Derecho Fundamental, así como de la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos.

A partir de ese momento, la RIPD se convirtió en un foro de promoción del Derecho Fundamental a la protección de datos en esta comunidad, cuyo impulso y responsabilidad asumieron también los responsables políticos de los respectivos Estados signatarios de la Declaración de Santa Cruz de la Sierra.

La consolidación definitiva de este foro como cauce idóneo para la toma de sus decisiones, adopción de documentos y fijación de sus estrategias futuras se convierte en uno de los objetivos estratégicos de la RIPD.

En definitiva, es interés primordial de las instituciones que en la actualidad constituyen la RIPD, el impulso e implantación del Derecho Fundamental a la Protección de Datos de Carácter Personal a través de las entidades con capacidad y competencias para instar a los gobiernos nacionales a que elaboren una regulación normativa en esta materia.

I. Objetivos de la RIPD

Artículo 1. Objetivos de la Red Iberoamericana de Protección de Datos.

1. Son objetivos de la RIPD:

a) Promover la cooperación interinstitucional y el diálogo entre actores claves para el desarrollo de iniciativas y políticas de protección de datos.
b) Promover políticas, tecnologías y metodologías que permitan garantizar el derecho fundamental a la protección de datos personales.
c) Brindar asistencia técnica y transferencia de conocimientos a los países iberoamericanos que así lo soliciten.

d) Promover convenios con instituciones públicas o privadas que permitan el desarrollo y ejecución de proyectos de su interés.
e) 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 sus actividades.
f) Participar en foros internacionales.
g) Dar transparencia y difusión universal a todas las actividades de la RIPD.
h) Promover programas de capacitación, orientación e información a los ciudadanos de cada país, acerca de las políticas de uso y destino de sus datos personales, así como de los derechos que puede ejercer frente al manejo que se haga de sus datos personales.

II. Organización de la RIPD

Artículo 2. Organización. – 1. La RIPD, se estructura en los siguientes órganos:

- Presidencia.
- Comité Ejecutivo.
- Secretaría.
- Encuentro Iberoamericano (EIPD).

2. Los miembros de la RIPD representarán a organismos públicos que contribuyan a promover, impulsar y tomar decisiones sobre las políticas de protección de datos personales y privacidad en sus países respectivos.

3. La adscripción a la RIPD se realizará mediante documento firmado por el interlocutor nacional correspondiente, donde se manifieste su interés por formar parte de la RIPD y asuma las funciones que como miembro de la misma se le atribuyan.

4. Cada país deberá elegir a una institución que realice la tarea de coordinación ante la RIPD de las distintas instituciones nacionales miembros de la RIPD. La institución coordinadora será considerada como interlocutor, sin perjuicio de que a los EIPDs puedan asistir representantes de las diferentes instituciones vinculadas y con competencias en dicha materia dentro de sus respectivos países.

5. La adhesión a este foro iberoamericano queda abierta a cualquier país del mismo entorno interesado en formar parte del mismo previa solicitud motivada dirigida a la Presidencia. La Secretaría, de acuerdo con los criterios y requisitos establecidos, instruirá las solicitudes de las que se dará cuenta en el siguiente EIPD.

6. En los Encuentros y seminarios podrán participar por invitación de la Secretaría observadores y expertos en materia de protección de datos.

Artículo 3. Presidencia. 1. La Presidencia de la RIPD será elegida por mayoría simple de entre los miembros presentes en el Encuentro de la RIPD.

2. Cada país ostentará un solo voto. La votación se realizará con motivo del correspondiente Encuentro Iberoamericano anual, una vez hayan transcurrido dos años desde el último Encuentro celebrado.

3. La Presidencia corresponderá a la persona que ocupe el puesto de dirección, presidencia o similar cargo en la Institución o Comisión Nacional de protección de datos personales del correspondiente país miembro de la RIPD. En caso de no existir dicha Institución o cargo, deberá ser elegido de entre las autoridades e instituciones nacionales competentes en dicha materia y siempre con categoría similar a la de aquellos.

4. La Presidencia será ocupada por un período de dos años, pudiendo renovarse por períodos iguales. En todo caso, ejercerá sus funciones hasta la nueva elección.

5. Corresponde a la Presidencia de la RIPD:

a) Representar a la RIPD en todos aquellos foros nacionales o internacionales en los que se traten aspectos relacionados con la protección de datos.
b) Promover y apoyar en las Cámaras Legislativas nacionales de los países del entorno iberoamericano todas aquellas iniciativas legislativas en proyecto.
c) Promover y representar a la RIPD ante los distintos actores sociales que operan en Iberoamérica y cuya actividad incida en este derecho fundamental.
d) Presidir las reuniones del Comité Ejecutivo.

6. La Presidencia podrá convocar, previa consulta a los miembros del Comité Ejecutivo, las reuniones que considere oportunas, a los efectos de debatir, analizar o resolver determinadas cuestiones que no pudieran esperar al siguiente Encuentro.

Artículo 4. Comité Ejecutivo. 1. El Comité Ejecutivo estará constituido por la Presidencia y cuatro Vocalías miembros de la RIPD.

2. Las personas que ocupen la Presidencia y las Vocalías no podrán representar al mismo país.

3. El mandato del Comité Ejecutivo tendrá la misma duración que el de la Presidencia, transcurrido el mismo y con motivo del siguiente Encuentro Iberoamericano, se elegirán a sus nuevos miembros.

4. El Comité Ejecutivo tendrá las siguientes funciones:

a) Asistir a los EIPDs y seminarios sectoriales que se celebren durante el ejercicio y decidir sobre los temas relacionados con el funcionamiento y las actividades de la RIPD.
b) Aprobar el programa de trabajo del siguiente ejercicio e impulsar todas las actuaciones necesarias para la celebración del próximo EIPD.
c) Aprobar la constitución de los Grupos de Trabajo.
d) Cooperar activa y periódicamente con la Secretaría en el desarrollo de las funciones que asuman.
e) Actuar como revisor editorial de las publicaciones presentadas.

5. Las reuniones del Comité Ejecutivo podrán celebrarse utilizando los medios tecnológicos adecuados que permitan el desarrollo de las mismas sin necesidad de que sus miembros tengan que desplazarse a otro país.

Artículo 5. La Secretaría. 1. La Secretaría de la RIPD se ejercerá por la Agencia Española de Protección de Datos, quién asumirá las tareas de coordinación como órgano técnico y de seguimiento de las actividades de la RIPD.

2. La Secretaría garantizará la continuidad institucional de las tareas y funciones de la RIPD.

3. La Secretaría de la RIPD asumirá las siguientes funciones:

a) Mantener una relación continua con el Comité Ejecutivo de la RIPD.
b) Establecer contactos con organismos nacionales e internacionales, instituciones afines y cooperantes a fin de gestionar posibles apoyos técnicos y logísticos para el desempeño de las actividades de la RIPD.
c) Llevar a cabo junto con los Grupos de Trabajo, el desarrollo de las decisiones y proyectos aprobados en los EIPDs.
d) Procurar una comunicación abierta e intercambio de información entre los miembros de la RIPD, atendiendo sus iniciativas y propuestas.
e) Coordinar las actividades de los Seminarios y Grupos de Trabajo.
f) Instruir las solicitudes de incorporación a la RIPD de nuevos miembros.
g) Convocar y colaborar en la organización de los EIPDs.
h) Tramitar las invitaciones de expertos y observadores a los EIPDs.

III. Encuentro Iberoamericano

Artículo 6. El Encuentro Iberoamericano (EIPD). 1. El Encuentro Iberoamericano es la Asamblea General de las Entidades miembros de la RIPD que se celebrará una vez al año y tendrá el carácter de órgano de la RIPD.

2.- El EIPD tendrá naturaleza de foro de discusión directa y de adopción de decisiones y documentos.

3. Los EIPDs determinarán los seminarios así como el programa de trabajo durante el año en curso, sin perjuicio de posibles iniciativas que pudieran surgir durante dicho período.

4. El EIPD elegirá por mayoría simple, de entre los miembros presentes, a la Presidencia.

IV. Grupos de Trabajo

Artículo 7. Grupos de Trabajo. 1. La conveniencia de analizar separadamente las materias objeto de cada EIPD y preparar los documentos de trabajo correspondientes puede aconsejar la creación de distintos Grupos de Trabajo, los cuáles desarrollarán un trabajo sistemático y especializado por temas.

2. Los Grupos de Trabajo estarán conformados por miembros de la RIPD y desarrollarán los trabajos y proyectos que en cada Encuentro se determinen, dependiendo su constitución de las materias que se les asignen así como de los países afectados e interesados.

3. Los Grupos de Trabajo podrán tener el carácter de temporales o permanentes de acuerdo con las actividades que desarrollen y según lo que se acuerde en los EIPDs.

4. Los Grupos de Trabajo deberán comunicar oportunamente a la Secretaría de la RIPD los avances en los documentos de trabajo que se les encomienden, y elevar los resultados de su trabajo ante el siguiente EIPD o ante los Seminarios correspondientes, dependiendo del contenido de los mismos.

Adoptado en Cartagena de Indias, a 30 de mayo de 2008.

.

ESTUDIO SOBRE EL DESARROLLO JURISPRUDENCIAL EN IBEROAMÉRICA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

definición de las categorías de clasificación de la jurisprudencia
Investigación sobre la génesis, planteamiento, deliberaciones y adopción de las jurisprudencias
análisis de los alcances jurídico interpretativo de los criterios jurisprudenciales

Comentarios preliminares

Valor del estudio

La protección jurisdiccional de la de la vida privada, la intimidad y mas especialmente de los datos personales ha tomado relevancia debido a la gran diversidad de conflictos que se presentan, en particular por el uso de soportes electrónicos y por la difusión en Internet. En efecto este es un terreno de gran innovación en el que las legislaciones no solo van a la zaga, sino también han mostrado una notable incapacidad para atrapar y prever los tipos de conflictividad que se presentan.

Dicho sea de paso, si los cuerpos legislativos durante años no han logrado incluir todos los tipos de conflictos y darles una solución normativa, tampoco se puede pretender que este estudio en escasos dos meses pueda reunir en un solo estudio toda esta diversidad, y describir o sintetizar en pocas líneas todo el conjunto de decisiones jurisdiccionales existentes en los países iberoamericanos.

El valor de este estudio es:

Resaltar la necesidad de utilizar la jurisprudencia comparada como fuente de inspiración para la toma de decisiones de cualquier órgano de impartición de justicia con competencia en la protección de los datos personales

Generar una primera aproximación a las líneas jurisprudenciales existentes en la región, como han cambiado en el tiempo y que paralelismos o líneas alternativas existen para dar solución a un mismo tipo de conflicto.

Favorecer el debate. En efecto los conflictos se presentan como destellos en los países de la región; ya por el hecho que son novísimos, pero aun más limitados por el acceso a la justicia para este tipo de conflictos. En efecto son conflictos que afectan al ciudadano de a pie, generalmente contra grandes corporaciones, y aun el el caso de ser vencedores las reparaciones pecuniarias son de mínima entidad. Es por ellos un área de escasa litigación. Si hay pocos litigios los jueces tienen muchas menos oportunidades de decir “cual es derecho en el caso”

Este contexto de lagunas normativas (muchas de ellas axiológicas) determina que los jueces e impartidores de justicia (muy frecuentemente en sede administrativa) sean llamados a crear normas. Los ciudadanos y las empresas necesitan normas para convivir con las nuevas tecnologías y con la innovación, si los legisladores no logran dar una respuesta útil y razonable, los impartidores de justicia y los mecanismos de autorregulación serán mirados con gran expectativa y sus soluciones serán determinantes.

En definitiva este estudio pretende clarificar y facilitar la labor jurisdiccional que realizan los órganos de impartición de justicia, fundamentalmente aquellos de gran acceso, como son las autoridades de protección de datos, que no solo deben resolver las cuestiones que le son presentadas, sino que pende sobre ellos la sombra de los tribunales que tienen la competencia de resisar sus decisiones, pues en algunos casos los jueces premian la creatividad y la interpretación integral de los derechos fundamentales y de los derechos humanos, pero en otros se refugian en la letra de la ley, fundamentalmente porque creen absolutamente mínimo —o temen— su papel constitucional de crear derecho.

Valor de la aplicación web

Este estudio se presenta en dos modalidades, un texto que pretende analizar todos y cada uno de los fundamentos, génesis y criterios de decisión utilizados en una selección —por cierto incompleta— de decisiones jurisdiccionales de algunos países iberoamericanos. Sin embargo es raro que un impartidor de justicia siga las decisiones que sugiere un libro. La gestación inconsciente de una decisión jurisdiccional es mucho más amplia que la simple referencia a la ley y la jurisprudencia. Como se verá en algunos ejemplos que se ponen más adelante, quien imparte justicia busca un equilibrio mucho mayor, que nace de forma intuitiva y busca —luego— fundamento en normas, jurisprudencia y derecho comparado.

El problema principal de un impartidor de justicia es la inspiración, saber hacia dónde inclinarse sabiamente, con visión de futuro; creando una línea jurisprudencial aceptada tanto por la comunidad. Como por sus colegas y académicos.

Esta tarea es extremadamente difícil, por la cantidad de casos que se deben resolver, los tiempos perentorios y la dificultad para obtener información pertinente.

Disponer de una base de jurisprudencia de los países de Iberoamérica es una herramienta muy valiosa. Porque ofrece la posibilidad de determinar si un tipo de conflicto ya ha sido resuelto en otro país, y cuál ha sido la solución. Si no existen referencias, habrán de buscarse analogías o criterios jurisprudenciales. El valor de sumar decisiones de distintos países, es aumentar la cobertura de conflictos y de sus soluciones en sistemas legales razonablemente análogos.

Un impartidor de justicia no busca una solución *a la carte,* busca inspiración, referencias, argumentos que pueda utilizar primero para definir su posición interior. En este punto es fundamental que la herramienta respete a raja tabla la “independencia” de quien imparte justicia.

Sobre estos argumentos se ha diseñado una plataforma informática para buscar decisiones jurisdiccionales capaces de iluminar la toma de decisión. La información allí colocada debe:

Ser imparcial y objetiva, deberá limitarse a incluir decisiones y clasificarlas evitando deslizar el menor prejuicio.

En ese sentido la herramienta ideal sería una base de jurisprudencia en la que es posible buscar en primer lugar por categorías fácticas. En segundo lugar la mejor herramienta es la búsqueda por texto. A diferencia de buscar en Internet, esta plataforma asegura la pertinencia

de las búsquedas. Claro está que buscar en Internet puede ser más productivo —y de ninguna manera se excluye— pero será necesario lidiar con toneladas de información basura.

La definición idiomática de la base de jurisprudencia está determinada por cierta intercambiabilidad lingüística que prescinde de la traducción para determinar pertinencia, y no requiere resolver problemas graves para la identificación de los conceptos.

En este sentido la base de jurisprudencia propuesta cuenta con un *caché* de los fallos encontrados para poder hacer búsquedas por palabras.[1]

La actualización y engrosamiento permanente de este tipo de herramienta es esencial, por ellos ha sido pensada en el contexto de la Red Iberoamericana de Protección de Datos Personales, comunidad que cuenta con capacidad y más especialmente con el clima de cooperación necesario para estos fines.

Es una primera aproximación. En efecto aquí no se agotan las necesidades de la RedIPD, sería fantástico dotar a esta plataforma con recursos para buscar noticias pertinentes, leyes, acuerdos de autorregulación y otro tipo de documentos con la capacidad de iluminar la relación entre conflictos y soluciones legales. O sea desarrollar un espacio de reflexión y al mismo tiempo un observatorio de la protección de datos en Iberoamérica.

Introducción

Para desarrollar este estudio se ha utilizado una selección de fallos jurisprudenciales de los países iberoamericanos que sirvan de base para encontrar los elementos distintivos de las decisiones en materia de protección de datos personales, vida privada, intimidad y habeas data.

Con esta finalidad los fallos han sido clasificados en categorías. La elección de las categorías hace a las diferentes formas de génesis, planteamiento, deliberación y adopción de las jurisprudencias; es decir tienen suficiente capacidad explicativa de porque se arriba a determinada solución jurídica.

Categorías

derechos

---

[1] **España** [17 Septiembre 2008] **[Audiencia Provincial de Barcelona - Sección 15]** **Recurso 749/2007 Aleix P. L., vs. Google Spain S.A.** Aleix P. L. compareció como titular de la web www.megakini.com para denunciar la violación de sus derechos de propiedad intelectual sobre dicha Web por parte de la demandada, GOOGLE SPAIN, S.A. (en adelante Google), quien, por medio de los sistemas de búsqueda, para incorporar una página a sus archivos realiza una copia de la misma, en la ubicación denominada **"caché"**, sin requerir la autorización del titular de la página copiada. “En nuestro caso, no consta, y ni siquiera fue alegado en la demanda, que Google haya infringido estas condiciones al prestar su "servicio caché""; respecto de la pagina web del actor, razón por la cual no cabe apreciar **ninguna infracción de los derechos de propiedad intelectual** del actor respecto de su obra contenida en dicha pagina Web, sin que el mero hecho de prestar ese servicio caché constituya una infracción del derecho de reproducción y de comunicación.”

- datos personales
- *habeas data*
- honor
- imagen
- intimidad
- olvido

personas

- fallecidas
- figuras públicas
- niños y adolescentes
- personas morales

tipo de datos

- ambiente laboral
- electorales
- historial crediticio
- Internet
- judiciales
- medios
- salud
- telecomunicaciones
- vigilancia

Líneas jurisprudenciales

Las líneas jurisprudenciales se construyen con la finalidad de identificar la aplicación en forma diferenciad de determinados criterios ya sea en el tiempo como entre países. De esta forma se puede apreciar que en un determinado país se ha cambiado la jurisprudencia en una fecha determina (o a partir de un fallo determinado), o los criterios son valorados en forma diferencial en diferentes países, generando así dos o más líneas paralelas.

Cada categoría da lugar entonces a varias líneas jurisprudenciales que se desarrollas en casos particulares o sub categorías.

Criterios jurisprudenciales

Los criterios son los principios jurídicos de fundamentación y argumentación para sostener cada una de las líneas jurisprudenciales advertidas. Se advierten algunos criterios que se reiteran en la mayoría de los fallos analizados, pero existen también otros que se aplican colateralmente o puntualmente en algunas decisiones.

Los criterios predominantes hallados son:

- **Ponderación de derechos**
- **Proporcionalidad del tratamiento**
- **Existencia de un interés público preponderante**
- **Consecuencias probables del tratamiento**
- **Tratamiento con fines de lucro**

El orden en que se han enumerado estos criterios predominantes no es casual, se relaciona con la jerarquía que se les atribuye en el razonamiento judicial, y obedece también al orden en que suelen ser aplicados por los jueces.

1. Líneas jurisprudenciales

categoría: **Derechos**

Como en todas las demás categorías analizadas, la selección no agota todas las posibilidades, es una primera aproximación para establecer más que nada paradigmas. También se eligen en función de los casos que han servido de base para este estudio, pero también con la pretensión de haber identificado conflictos nuevos que ponen en jaque las decisiones tomadas en el pasado.

Derecho: **datos personales –** caso: **pseudónimos.** El criterio jurisprudencial es mayormente ajustarse al texto **legal** y la principal dificultad en estos casos consistiría en el ejercicio del el **derecho de oposición**.

El uso de pseudónimo se ha convertido en una necesidad, incluso es recomendado a los niños y adolescentes para identificarse en Internet. Sin embargo existe muy poca regulación.

Existe en el derecho una asimetría o diferenciación entre las personas físicas y las personas morales respecto del cambio de nombre. A las personas jurídicas les es permitido libremente dicho cambio mucho más fácilmente

Américas [18 Agosto 2003] **[Tribunal de Justicia de la Comunidad Andina] Interpretación prejudicial 57-IP-2003 Floristería Jardín Kennedy** De conformidad con el artículo 83, literal f, de la Decisión 344 no son registrables los nombres completos, ni el apellido, ni el seudónimo, ni la firma, ni tampoco la caricatura o el retrato de personas naturales distintas del peticionario o, que sean identificadas por la generalidad del público como distintas a él, salvo que medie su consentimiento o el de sus herederos. La titularidad de los derechos para oponerse al registro o para solicitar su anulación en caso de que se haya producido, se radica en cabeza de las personas naturales portadoras del nombre propio protegido o del apellido, o dueñas del seudónimo o de la firma o sujetos de la caricatura o del retrato. Puede radicarse también en cabeza de sus herederos, de conformidad con lo que disponga la legislación nacional correspondiente.

No se han identificado casos en los que una persona se oponga a la utilización de su nombre como pseudónimo por parte de otra (que llevaría a discutir el grado de protección que tiene

en nombre propio). La sentencia del Tribunal Andino si pone limitaciones para las personas morales.

La vinculación entre nombre real y pseudónimo no se considera protegida:

Chile [10 Abril 2006] **[Corte de Apelaciones de Santiago - Tercera Sala]** **Rol Nº 981-2006** La mera divulgación, efectuada por TVN, de la identidad del personaje Ruperto, a juicio de esta Corte, no menoscaba, en absoluto, la reputación de Ch. H., como para impetrar la presente acción tutelar, cuya acogida atentaría gravemente contra un derecho humano fundamental: difundir informaciones e ideas, cuyo ejercicio no puede estar sujeto a previa censura sino a responsabilidades ulteriores, como lo señala la Convención Americana sobre Derechos Humanos o también llamado Pacto de San José de Costa Rica

En **Argentina** y **Paraguay** la jurisprudencia no acepta el reemplazo del pseudónimo por el nombre.

En **Argentina** [02 Octubre 2009] **[Cámara Nacional de Apelaciones en lo Civil - Sala G]** **L., J.L vs. L., N.A.**, la sentencia dictada en primera instancia había hecho lugar a la demanda de impugnación de paternidad matrimonial promovida por J.L.P. contra N.A.P y N.G.G. y dejó sin efecto la filiación paterna establecida en la correspondiente partida de nacimiento respecto de J.L.P. por no ser hijo de N.A.P. e impuso al actor el apellido J.L, agregando que el estudio del polimorfismo de ADN practicado había concluido que N.A.P. no podía ser padre biológico de J.L.P.

El actor había requerido, y la sentencia recurrida ha admitido, que se anteponga el vocablo J. al apellido L. invocando que todos lo conocen con ese apellido (J), explicando que desde pequeño fue conocido con el "seudónimo" de J., derivado de su primer nombre de pila J., siendo desde su adolescencia hasta la actualidad su apellido, alegando el actor que el mismo lo identifica en su grupo íntimo, como así también en el social, profesional y en todo su mundo de relación.

[2 de octubre de 2009] **Argentina** [Cámara Nacional Civil - Sala G] revocó la resolución recurrida señalando que resultaba inadmisible la pretensión del actor, debido a que no había logrado demostrar el uso notorio como tal del vocablo por el que pretende cambiarlo, sino más bien quedó demostrado que ha sido un apodo o sobrenombre, en el sentido de constituir una designación espontánea producida en el estrecho ambiente familiar, social y propia del círculo de sus íntimos, aunque muchas veces lo hubiese trascendido confundiéndose con su nombre propio.

Paraguay [2005] **[Asunción - Tribunal de Apelación en lo Civil y Comercial, Tercera Sala]** **I.S.C.C.** Un seudónimo es protegido por la ley con la misma fuerza que el nombre, pero que no puede ser confundido con el mismo; y que se diferencia de él por la posibilidad de cambiarlo e incluso cederlo. Por ello, citando doctrina, reconoce la importancia y función individualizadora reconocida incluso por el Código Civil, pero niega la posibilidad de equipararlo al nombre civil, hecho que entiende prohibido por legislación de orden público.

Notas legislativas:

> En Argentina la Ley del Nombre de las Personas Naturales establece en el artículo 24 que "cuando el seudónimo hubiere adquirido notoriedad, goza de la tutela del nombre."

En Paraguay en ese mismo sentido se le tutela por el Código Civil en el numeral 47.

En **México**, el Código Civil del estado de Jalisco define, en el artículo 67, al seudónimo, pero no establece si tiene protección como el nombre. El Estado de Coahuila establece en el numeral 70, del Código Civil que "el derecho a usar nombre o seudónimo es imprescriptible" y en el diverso 66 determina que "toda persona tiene derecho al uso ... del seudónimo, cuando éste desempeñe realmente la función del nombre".

Colombia: Decreto 1260 de 1970 (Julio 27) Por el cual se expide el Estatuto del Registro del Estado Civil de las personas.

> **Artículo 3.** Toda persona tiene derecho a su individual, y por consiguiente, al nombre que por ley le corresponde. El nombre comprende, el nombre, los apellidos, y en su caso, el seudónimo.
>
> No se admitirán cambios, agregaciones o rectificaciones del nombre, sino en las circunstancias y con las formalidades señaladas en la ley.
>
> El juez, en caso de homonimia, podrá tomar las medidas que estime pertinentes para evitar confusiones.
>
> HECHOS Y ACTOS SUJETOS A REGISTRO
>
> **Artículo 5.** Los hechos y los actos relativos al estado civil de las personas, deben ser inscritos en el competente registro civil, especialmente los nacimientos, reconocimientos de hijos naturales, legitimaciones, adopciones, alteraciones de la patria potestad, emancipaciones, habilitaciones de edad, matrimonio, capitulaciones matrimoniales, interdicciones judiciales, discernimientos de guarda, rehabilitaciones nulidades de matrimonio, divorcios, separaciones de cuerpos y de bienes, cambios de nombre, declaraciones de seudónimos, manifestaciones de avencidamiento, declaraciones de ausencia, defunciones y declaraciones de presunción de muerte, así como los hijos inscritos, con indicación del folio y el lugar del respectivo registro.

Doctrina: Joan Steinman, Litigios bajo pseudónimo en los EE.UU. — una puesta al día

Doctrina: María Aurora Lacavex Berumen, El nombre de las personas físicas

Derecho: ***habeas data***

Existen diferencias en la región sobre la valoración del término habeas data. Mientras que en Colombia cubre todos los aspectos de la protección de los datos personales, en Argentina es visto solo como la acción procesal.

Argentina [14 Septiembre 1999] **[Corte Suprema] G., M. F. y otra, hábeas corpus** A los efectos de la acción de "hábeas data", la Constitución Nacional prevé que las informaciones deben constar en registros o bancos de datos públicos, es decir que la información debe ser pública o

al alcance de los particulares. De esta forma, no procede la acción en relación a la información obrante en los registros de las fuerzas y organismos de seguridad, pues no reviste el carácter público por obvias razones de seguridad pública. (CNCrim. y Correc., Sala de feria, agosto 3-991. "G., M. E. y otra s/hábeas corpus y hábeas data". Revista La Ley, 21/05/1998).

Colombia [01 Junio 2001] **[Corte Constitucional - Sala Quinta de Revisión]** **Sentencia T-578-01** ... el derecho fundamental establecido en el artículo 15 de la Constitución, ha señalado esta Corporación en muchas oportunidades, que el habeas data es el derecho que tienen todas las personas a *"conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas"*.

Las sentencias en Colombia son inclusivas de las definiciones de los términos jurídicos. En **Colombia** [08 Mayo 2000] **[Corte Constitucional - Sala Séptima de Revisión]** **Sentencia T-527-00** se hace una amplia descripción del uso del concepto *habeas data*.

En **Costa Rica** [27 Julio 1999] **[Corte Suprema - Sala Constitucional]** **Sentencia 5802/1999** Se define la naturaleza del recurso de hábeas data, y el el ámbito de tutela de este instrumento: *a.) Derecho al acceso; b.) Derecho a la actualización; c.) Derecho a la confidencialidad; d.) Derecho a la exclusión; e.) Derecho de inserción; f.) Derecho a saber del conocimiento de terceros sobre la información recolectada.*

Derecho: **honra –** caso: **difamación**

Las decisiones por difamación se por **ponderación de derechos** entre a la honra y la libertad de expresión. Muchas legislaciones se han reformado para excluir sanciones penales que ahogarían la libertad de expresión y crearían persecución contra los periodistas, por eso se resuelve con sanciones civiles. Cuando la expresión es anónima, en algunos países los jueces deslizan la responsabilidad civil a los proveedores (esta opción está limitada en los EE.UU. si la responsabilidad es por contenidos). En Argentina, Brasil y recientemente en España se están generalizando las condenas civiles por expresión anónima, al propietario del blog, al periódico que permite la publicación instantánea o al proveedor de conectividad. La jurisprudencia de Brasil es novedosa al condenar por "**responsabilidad por productos**" en logar de responsabilidad por "contenidos" y en utilizar también el criterio de "**consecuencia probable**" de la expresión anónima, y "**tratamiento con fines de lucro**"

Las decisiones por difamación se resuelven ponderando los derechos a la honra y el de libertad de expresión. Muchas legislaciones se han reformado para excluir sanciones penales que ahogarían la libertad de expresión y crearían persecución contra los periodistas.

Los procesos judiciales por difamación se han convertido en una de las discusiones centrales sobre Internet como espacio de libertad. Muchas plataformas de sociabilización, blogs, o la posibilidad de hacer comentarios a una nota periodística, ponen en manos de cualquier internauta la posibilidad de publicar inmediatamente un texto en la red. Esto es visto como un avance en términos de libertad de expresión.

Que la expresión sea anónima es también parte de la garantía de libertad de expresión (quizás con la excepción de Brasil, donde la Constitución garantiza el derecho a expresarse pero excluye la expresión anónima). Si la expresión es anónima, y el contenido es ofensivo a la honra de una persona se presenta entonces la dificultad de cómo poner en equilibro la libertad de expresión con el derecho a la honra, a la intimidad o a la imagen.

En los EE.UU. (situación explicable desde la integralidad de las normas vigentes, en las que unas compensan a las otras, al igual que los mecanismos de *law enforcement*). El tema es visto con una visión diferente. En [05 Octubre 2005] **[EE.UU. - Supreme Court of the State Of Delaware] John Doe vs. Patrick Cahill** se debe probar primero la difamación, y entonces el juez autoriza que el proveedor del servicio de conectividad revele las pistas que permitan identificar al usuario.

En los EE.UU. es mucho más probable la identificación, que en otros países en donde la conexión predominante es en *ciber-cafes*.

Existen muchas decisiones en Brasil como esta: **Brasil** [12 Febrero 2009] **[Minas Gerais - Tribunal de Justiça do Estado - 13ª Câmara Cível] R. S. B. v. Google do Brasil Internet Ltda.**

Existen algunas notas características en estos procesos judiciales: (1) se inician en juzgados de menor cuantía denominados en Brasil *Juizados Especiais*, sin formalidades, no requieren el patrocinio de un abogado y no existen costas judiciales. El damnificado presenta una demanda contra un usuario de *Orkut* que solo conoce por un *nickname* (pseudónimo o nombre de fantasía) y subsidiariamente contra *Google* para que revele la identidad del usuario; (2) el juez libra una orden a *Google* para que informe la identidad del usuario detrás del nombre de fantasía bajo una pena de 5.000 reales por día mientras no satisfaga esta información.[2]

En primer lugar *Google* adujo que los usuarios aceptaban los tribunales de los EE.UU. al adherir como usuarios de *Orkut*; la respuesta de la justicia de Brasil fue que esa aceptación es nula y que la jurisdicción de los tribunales brasileños es irrenunciable. En segundo lugar *Google do Brasil* (a quien estaban dirigidas las demandas) argumentó ser solo una oficina de representación; la justicia brasileña respondió que el uso del nombre *Google* y su calidad de representación, así como la capacidad para recolectar los pagos de los servicios de publicidad la hacían solidariamente responsable, y por tanto podía ser desmanda.

En una importante cantidad de casos *Google do Brasil* no ha podido identificar a la persona física detrás de los perfiles, entonces los jueces condenaban a *Google de Brasil* a pagar los daños morales que rondan los 10.000 reales por caso.

Los argumentos de *Google* frente a las decisiones judiciales en Brasil se remiten a la sección 230 de la *Communications Decency Act* de los EE.UU. en la que los proveedores son inmunes frente a acciones judiciales por contenidos —denominada protección para el *buen samaritano*.[3] Sin embargo las condenas en Brasil son por la responsabilidad derivada de productos elaborados, aplicaciones que incluyen la posibilidad de operar en forma anónima, y

[2] Esta es una multa media, hay algunas variaciones de un juzgado a otro; equivale a unos 2.000 euros por día. No en todos los casos *Google do Brasil* es el demandado, también existen casos contra *Fotolog* y *Facebook* y contra personas físicas cuando son identificables.

[3] www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230----000-.html

no necesariamente por un contenido en particular; debe tenerse en cuenta adicionalmente que la Constitución Política de Brasil garantiza la libertad de expresión pero excluye el anonimato.

Derecho al buen nombre – honra

De acuerdo con la línea jurisprudencial actualmente vigente en Colombia, los historiales crediticios no son vistos desde el derecho a la intimidad sino desde el derecho al buen nombre o del derecho a la honra:

Colombia [02 Marzo 1995] **[Corte Constitucional - Sala Quinta de Revisión]** **Sentencia T-094/95** En cuanto a los derechos a la honra y al buen nombre, resultan afectados cuando el banco de datos recoge, maneja o difunde informaciones falsas o cuando, en el caso de las verdaderas, lo sigue haciendo no obstante haber caducado el dato, según los criterios de razonabilidad señalados por la doctrina constitucional.

Derecho: **imagen**

España [16 Abril 2007] **[Tribunal Constitucional - Sala Primera]** **Sentencia 072/2007** El derecho a la propia imagen no es absoluto o incondicionado, de suerte que existen circunstancias que pueden determinar que la regla general conforme a la cual es al titular de este derecho a quien, en principio, corresponde decidir si permite o no la **captación y difusión de su imagen por un tercero**, ceda a favor de otros derechos o intereses constitucionalmente legítimos, lo que ocurrirá en los casos en los que exista un **interés público** en la captación o difusión de la imagen y este interés público se considere **constitucionalmente prevalente** al interés de la persona en evitar la captación o difusión de su imagen. Por ello, cuando el derecho a la propia imagen entre en colisión con otros bienes o derechos constitucionalmente protegidos, particularmente las **libertades de expresión e información** [art. 20.1 a) y d) CE], deberán ponderarse los distintos intereses enfrentados y, atendiendo a las **circunstancias concretas de cada caso**, decidir qué interés merece mayor protección, si el interés del titular del derecho a la imagen en que sus rasgos físicos no se capten o difundan sin su consentimiento o el interés público en la captación o difusión de su imagen (STC 156/2001, de 2 de julio, FJ 6).

España [09 Julio 2009] **[Audiencia Nacional - Sala de lo Contencioso]** **SAN 3658/2009** es un ejemplo de ponderación a favor de la libertad de expresión.

La imagen —a diferencia del nombre— puede ser licenciada contractualmente.

Brasil [08 Abril 2005] **[Tribunal Regional de Trabajo de la 15ª Região]** **Decisão 013966/2005-PATR**. Ainda que o uso da imagem não traga danificação à personalidade e a integridade moral da pessoa, a inviolabilidade da intimidade da vida privada, representada pela publicação de fotografia com fins comerciais, sem autorização do fotografado, caracteriza-se como locupletamente ilícito à custa de outrem, o que importa em indenização por reparação ao

dano causado. Inteligência dos artigos 5º, inciso X da Constituição Federal da República, c/c. os artigos 18, 20 e 186 do Novo Código Civil Brasileiro.

La indemnización por daño moral es el instrumento de protección del derecho a la imagen, en este caso se quiebra la magnitud del lucro obtenido por el medio con el valor económico de la imagen. **Brasil** [15 Marzo 2011] **[Superior Tribunal de Justiça - Quarta Turma] Recurso Especial 2010/0165995-6** Cuidando-se de pessoa anônima, **a vinculação da indenização por uso da imagem ao percentual do preço de venda do veículo no qual a imagem foi publicada**, de regra, não é consentânea com a essência de indenizações desse jaez. **Indeniza-se o titular do direito de imagem pelo não-recebimento do preço que lhe seria devido, caso a concessão fosse feita mediante autorização, e pelo respectivo valor econômico da imagem, que varia a depender do potencial publicitário da pessoa retratada.**

El uso de la imagen no puede considerarse parte del contrato laboral, además la indemnización por daño moral se incrementa al tener en cuenta la inferioridad económica del empleado y el miedo al desempleo.

Brasil [20 Abril 2006] **[Tribunal Regional de Trabajo de la 15ª Região] Decisão Nº 016299/2006-PATR .** A utilização da imagem do empregado pelo empregador não pode ser subentendida como decorrente do contrato de trabalho, que não produz efeitos tão amplos, pena de gerar locupletamento ilícito; o uso da imagem pode ser ajustado, mas não deflui originariamente do contrato laboral; de maneira que frágil falar-se, na hipótese, de anuência presumida. Indenização devida.

Por fim, quanto a esse tópico, cumpre notar que a ofensa moral, em sede trabalhista, praticada ou permitida pelo empregador, é de ser considerada mais grave do que se cometida em outras situações, ou, pelo menos, em algumas outras situações, pois traduz abuso ou descaso reprovável, diante da inferioridade econômica do trabalhador e do pavor do desemprego, podendo mesmo, em determinados casos, resvalando para ato de desumanidade, o que, por seu turno, deve, também, ser considerado, na e para a fixação da indenização.

> **Doctrina**: Sérgio Ferreira Pantaleão dice que "O direito de imagem é um direito personalíssimo e negociado diretamente entre o jogador (ou a empresa que o detém) com a entidade desportiva (clube de futebol), por meio de valores e regras livremente estipulados entre as partes, assegurado pelo art. 5º, XXVIII, "a", da Constituição Federal.
>
> Embora seja cada vez mais comum os atletas venderem a sua imagem a patrocinadores e a marcas, cabe ressaltar as implicações legais deste tipo de contrato. Como mencionado no parágrafo anterior, o direito à imagem, garantido pela Constituição Federal, pertence ao rol de Direitos da Personalidade, caso em que deve ser assegurado intacto o direito à intimidade da vida privada."
>
> Sérgio Ferreira Pantaleão, Jogador profissional - direito de arena e direito de imagem

Derecho: **intimidad** – caso: **revisión abusiva y vejatoria**

La revisión personal o de los bienes de una persona por razones de seguridad (u otro derecho) es enmarcado por los jueces haciendo una **ponderación de derechos**. En primer lugar

consideran el derecho que se busca proteger. Luego se realiza una valoración para establecer si la revisión es **proporcionada** con los riesgos, si es eficaz al considerar las molestias y si es necesaria. Agotada esta ponderación en algunos casos también analizan las **consecuencias probables** que puede producir alguna característica de la revisión (revelación de datos, higiene, etc.).

En relaciones de consumo: se considera desproporcionada si no se realiza en privado: **Argentina** [02 Diciembre 1999] **[Santa Fe - Cámara Civil y Comercial de Rosario] B. H., R. vs. Carrefour Rosario**. En este caso fue desproporcionada (sin la delicadeza necesaria) y generó consecuencias (ridiculización por parte de otras personas). La condena es por daño moral.

No resiste la ponderación si solo se busca proteger la propiedad intelectual: [15 Febrero 2011] **[Canadá - Quebec] Cinémas Guzzo inc. c. Berthiaume**. En este caso se hace preliminarmente una ponderación de derechos entre intimidad y derechos de autor, y el juez opta por la intimidad, también juzga desproporcionada la revisión y con consecuencias (ver: **niños y adolescentes**)

En ambiente laboral:

La revisión sin contacto físico en ambiente laboral no se considera lesiva de la intimidad:

Brasil [16 Noviembre 2011] **[Tribunal Superior do Trabalho] TST-RR-8800-65.2008.5.19.0007**

Que un empleado deba desnudarse ante su jefe y en presencia de sus compañeros se considera desproporcionada: **Brasil** [16 Noviembre 2011] **[Tribunal Superior do Trabalho] TST-RR-18540-38.2006.5.01.0033**

En algunas decisiones se requiere para una revisión intima “sospecha razonable”

> Doctrina: **Brasil** - Pedro Henrique Holanda Pucci, Meios e cautelas da revista de empregados de acordo com a jurisprudência dos tribunais

En aeropuertos:

> [13 Abril 2011] [nota de prensa] Polémica revisión a una niña de seis años en un aeropuerto de EE.UU.

En edificios públicos:

Costa Rica [12 Noviembre 2010] **[Corte Suprema - Sala Constitucional] Sentencia 18.874/2010** - **revisión de visitantes en el poder judicial.** Argumenta el recurrente que se presentó al edificio de los Tribunales del Segundo Circuito Judicial de San José y que los oficiales de seguridad lo forzaron a levantar las manos, para pasar por su cuerpo un aparado para desconocidas verificaciones, así también lo obligaron a vaciar los bolsillos y abrir y mostrarles el contenido de su maletín. Reclama que la requisa de la cual fue objeto fue denigrante; el trato de los oficiales de seguridad fue altanero y prepotente. Ellos se arrogan la potestad de decidir quién ingresa o no a las oficinas judiciales, sin que exista razón fáctica ni jurídica para obligar a los usuarios del servicio de administración de justicia a requerir su aprobación. Con base en las consideraciones dadas en la sentencia, se declara sin lugar el recurso.

En escuelas:

> **México** [28 Septiembre 2011] [nota de prensa en] La directora de un colegio obliga a 20 niños a desnudarse para buscar 13 dólares. Este caso fue resuelto por la Comisión de Derechos Humanos del Estado de Michoacán.

En visita de cárceles:

Mientras que en **Colombia** se ponderan derechos en **Brasil** se valoran consecuencias:

Colombia [16 Agosto 2005] **[Corte Constitucional] Sentencia T-848/05** (1) El Estado tiene la legítima facultad y obligación para practicar requisas razonables y proporcionadas, legalmente consideradas. (2) En el caso de los visitantes, específicamente, toda persona que ingrese a un centro de reclusión o salga de él, por cualquier motivo, deberá ser razonablemente requisada y sometida a los procedimientos de ingreso y egreso; por gozar los visitantes de la plenitud de sus derechos, sólo pueden ser razonables las limitaciones que sean necesarias, para obtener el fin buscado. (3) En cualquier caso, no es razonable una requisa que se realice transgrediendo el derecho a la dignidad humana de la persona (reclusa o visitante) al manipular sus partes íntimas, cuando no es necesaria por existir otros mecanismos para garantizar la seguridad. (4) No es razonable constitucionalmente, por implicar una violación al derecho fundamental a no ser sometido a tratos crueles, inhumanos o degradantes, las requisas intrusivas que son practicadas por la guardia de un establecimiento de reclusión, tales como desnudar al recluso o al visitante, obligarlo a agacharse o a hacer flexiones de piernas y mostrar sus partes íntimas a la guardia; más aún si éstas se practican en condiciones insalubres. (5) Las intervenciones, registros, injerencias, comprobaciones o extracciones sobre los cuerpos, tales como las 'requisas intrusivas', pueden llegar a darse por razones fundadas "(…) siempre que medie el consentimiento informado del afectado y el registro se practique de modo que el pudor y el decoro personal no resulten ofendidos, ni la integridad física y jurídica vulnerada, condicionamientos éstos que demandan (i) un mandato legal, (ii) la supervisión judicial, (iii) la intervención de personal experto y (iv) el uso de instrumental y condiciones sanitarias adecuadas, porque los tratos crueles, inhumanos y degradantes están proscritos y su prohibición es absoluta".

Brasil [17 Diciembre 2009] **[Superior Tribunal de Justiça - Segunda Turma] Recurso Especial Nº 712.258 - RS (2004/0179060-8)**

REVISTA PESSOAL DAS VISITAS FEITAS À POPULAÇAO CARCERÁRIA - Encontra-se dentro do limite da razoabilidade a imposição de restrição, ainda que incômoda, em prol de bem jurídico maior e mais abrangente - a segurança pública em geral e a dos presídios, em específico -, constituindo-se o ato em típico exercício do regime jurídico de sujeição especial que rege o vínculo entre os detentos e a administração penitenciária.

España [16 Diciembre 1996] **[Tribunal Constitucional - Sala Primera] Sentencia 207/1996**
Una vez constatada la afectación por la intervención corporal y consiguiente pericia de los derechos fundamentales a la integridad física y a la intimidad personal, hemos de concretar ahora si el sacrificio de tales derechos fundamentales es susceptible de alcanzar una justificación constitucional objetiva y razonable. A tal efecto, conviene recordar los requisitos que conforman nuestra doctrina sobre la **proporcionalidad**, los cuales pueden resumirse en los

siguientes: que la medida limitativa del derecho fundamental esté prevista por la Ley, que sea adoptada mediante resolución judicial especialmente motivada, y que sea idónea, necesaria y proporcionada en relación con un fin constitucionalmente legítimo. A todos ellos hay que sumar otros derivados de la afectación a la integridad física, como son que la práctica de la intervención sea encomendada a personal médico o sanitario, la exigencia de que en ningún caso suponga un riesgo para la salud y de que a través de ella no se ocasione un trato inhumano o degradante.

6. Para que una intervención corporal en la persona del imputado en contra de su voluntad satisfaga las exigencias del principio de proporcionalidad será preciso: a) que sea idónea (apta, adecuada) para alcanzar el fin constitucionalmente legítimo perseguido con ella (art. 18 C.E.D.H.), esto es, que sirva objetivamente para determinar los hechos que constituyen el objeto del proceso penal; b) que sea necesaria o imprescindible para ello, esto es, que no existan otras medidas menos gravosas que, sin imponer sacrificio alguno de los derechos fundamentales a la integridad física y a la intimidad, o con un menor grado de sacrificio, sean igualmente aptas para conseguir dicho fin; y c) que, aun aun siendo idónea y necesaria, el sacrificio que imponga de tales derechos no resulte desmedido en comparación con la gravedad de los hechos y de las sospechas existentes.

Comisión Interamericana de Derechos Humanos [13 Marzo 2008] Resolución 1/08 - Principios y buenas prácticas sobre la protección de las personas privadas de libertad en las Américas

Principio XXI
Registros corporales, inspección de instalaciones y otras medidas

> Los registros corporales, la inspección de instalaciones y las medidas de organización de los lugares de privación de libertad, cuando sean procedentes de conformidad con la ley, deberán obedecer a los criterios de necesidad, razonabilidad y proporcionalidad.
>
> Los registros corporales a las personas privadas de libertad y a los visitantes de los lugares de privación de libertad se practicarán en condiciones sanitarias adecuadas, por personal calificado del mismo sexo, y deberán ser compatibles con la dignidad humana y con el respeto a los derechos fundamentales. Para ello, los Estados Miembros utilizarán medios alternativos que tomen en consideración procedimientos y equipo tecnológico u otros métodos apropiados.
>
> Los registros intrusivos vaginales y anales serán prohibidos por la ley.
>
> Las inspecciones o registros practicados al interior de las unidades e instalaciones de los lugares de privación de libertad, deberán realizarse por autoridad competente, conforme a un debido procedimiento y con respeto a los derechos de las personas privadas de libertad.

derecho: **al olvido**

Colombia [07 Julio 2003] **[Corte Constitucional - Sala Octava de Revisión] Sentencia T-592-03**
DERECHO AL OLVIDO - Restablecimiento del buen nombre e intimidad Quien con el

cumplimiento de sus obligaciones logra crear un nombre que en el pasado no ostentó, tiene derecho a exigir que su esfuerzo se refleje en la información que se divulga sobre él, planteamiento éste sostenido por diversas Salas de Revisión, al considerar que “las sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia, después de algún tiempo tales personas son titulares de un verdadero derecho al olvido". Pero el derecho al olvido, a fin de restablecer el buen nombre, no es lo único que cuenta en la definición de los límites de permanencia de los datos adversos en los ficheros de datos, también la dignidad del deudor reclama que la valoración de su conducta se realice en consideración a su condición humana, en función de la cual las personas pueden en todo tiempo recuperar su nombre e intimidad por haber enmendado su conducta.

La permanencia sin límites de los datos adversos a los usuarios del crédito en el proceso informático constituye un abuso de la autorización recibida –artículo 95 C.P.-, y no cumple con el presupuesto de informar con responsabilidad social –artículo 20 C.P. amén de que colisiona i) con la facultad del titular de la información de autodeterminarse, mediante la actualización o eliminación de sus datos del proceso, salvaguardando así su intimidad económica y el derecho a su buen nombre, y ii) con la dignidad humana de quien enmienda su comportamiento mejorando sus hábitos de pago –Preámbulo, artículos 1°, 2°, 5°, 13, y 15 C.P. Finalmente, en punto al poder resarcitorio del tiempo, es evidente que el Legislador no permite pactar sumas compensatorias que excedan el doble de la obligación principal, límite éste que permite a la Sala considerar el duplo de la mora, como criterio válido de permanencia de un dato adverso en el proceso informático, acudiendo a los artículos 1601 y 867 de los Códigos Civil y de Comercio, respectivamente. Es decir que, para conjurar la conservación de la información negativa, al titular de ésta le basta la extinción de la obligación que dio lugar a ella, más el acaecimiento de un plazo igual al de la permanencia inicial del dato adverso, contada a partir de la mora. O sea que, en tanto el Legislador regula específicamente el asunto, conforme lo indican las disposiciones antes referidas, al parecer de la Sala, las centrales de riesgo, haciendo uso de la autorización de su titular, podrán, a partir de la mora, procesar y divulgar informaciones sobre obligaciones insolutas, hasta su extinción, tiempo éste al que se podrá agregar hasta uno más. LEGISLADOR-Necesidad de reglamentar el proceso informático en relación con el dato negativo Dado el vacío legal respecto de la permanencia del dato negativo en las centrales de riesgo, esta Corporación ha venido insistiendo en la necesidad de que el legislador determine de manera general como le corresponde, qué debe entenderse por dato adverso y por cuánto tiempo éste puede permanecer en el proceso informático, habida cuenta que la competencia de esta Corporación al respecto se circunscribe a “ejercer el control de constitucionalidad sobre la ley que reglamente este derecho (..)"

El derecho al olvido es reconocido cuando está legislado, y también es reconocido por la vía jurisprudencial **Costa Rica** [14 Octubre 2008] **[Corte Suprema - Sala Costitucional]** **Sentencia 15.421/2008** Sentencia que resuelve recurso de amparo en el cual el recurrente reclama como vulnerados sus derechos a la intimidad y vida privada, debido a que la sentencia mediante la cual fue condenado a una pena de prisión por tentativa de homicidio, la cual cumplió, aparece publicada en la página Web del Poder Judicial con su nombre y apellidos, y puede ser accedida mediante cualquier buscador de Internet. El recurrente solicita se elimine de la red cualquier documento en el que aparezca su nombre y apellido referente al expediente judicial. Se señala "la publicidad de la sentencia a que se refiere el recurrente no

vulnera los plazos previstos en la Ley del Registro y Archivos Judiciales No. 6723 del 10 de Marzo de 1982, que señala los plazos de vigencia de los asientos en que consten las condenatorias penales, a fin de que tales sanciones no tengan un efecto perpetuo prohibido por la Constitución"

Sin embargo la mayor dificultad para garantizar el derecho al olvido es la "cesión indiscriminada" que significa la publicación en Internet. Los datos publicados en internet quedan fueran de control, pueden y son almacenado por repositorios masivos en forma automática, como por ejemplo www.archive.org.[4]

categoría: **Personas**

Tipo de persona: **fallecidos**

Los casos se resuelven por **ponderación de derechos**, aun cuando se ponderen contra un "diluido derecho a la intimidad". Se aplica legalidad sobre el vínculo familiar o de relación requerido para acceder a la historia clínica. Se menciona la ponderación con el acceso a la justicia si se pretende iniciar una acción por responsabilidad médica.

Filiación

Chile, se hace una ponderación entre derechos y se analiza el pretendido concepto de "privacidad familiar"

Chile [06 Octubre 2010] **[Corte de Apelaciones de Temuco - Segunda Sala] N° 1395-2010-PROT** Que la privacidad familiar alegada, no puede ir por sobre el derecho de un probable hijo no matrimonial del causante, a investigar su filiación, lo que atentaría contra el principio de igualdad ante la ley.

3°.- Que tampoco puede estimarse vulnerada la intimidad familiar, en circunstancias que se encuentra judicializada la gestión de reconocimiento de paternidad, lo que ya implica que una intimidad con tal grado de secretismo, ya no existe.

4°.- Que el uso del ADN en los estudios de vínculos de parentesco debe basarse, necesariamente y de acuerdo al Servicio Médico Legal, con muestra de sangre del presunto padre fallecido y, si no, es el caso, realizar una exhumación del presunto padre y disponer de muestra ósea, que es lo que la Juez de primer grado ordenó.

[4] Internet Archive's web archive, launched in 1996, contains over 2 petabytes of data compressed, or 150+ billion web captures, including content from every top-level domain, 200+ million web sites, and over 40 languages. The Internet Archive, a 501(c)(3) non-profit, is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public.

5°.-Que nadie discute ni niega la justicia que encierra el aceptar la investigación de la paternidad que en forma más amplia o restringida consagran todas las legislaciones (Evolución del Código Civil Chileno, pág.143).

Datos de salud del fallecido - Protección de datos personales que subsiste a la muerte:

Colombia [29 Enero 2009] **[Corte Constitucional - Sala Septima de Revisión]** **Sentencia T-044/09** … en el caso bajo estudio estamos frente a un diluido derecho a la intimidad, siendo de recordar que la existencia de la persona se termina con la muerte (art. 94 Código Civil), sin perjuicio de que pervivan sentimientos merecedores de respeto. Con todo, no resultando necesario ante el caso concreto profundizar sobre cuáles derechos fundamentales terminan, y de qué manera, con la muerte de su titular, sí es claro que esta específica expresión de la intimidad no es oponible por la [clínica demandada] a la justa aspiración del hijo accionante. ...

Se reconoce el derecho de acceso a la historia clínica frente a una intimidad diluida del fallecido, de acuerdo con la ley (en función del parentesco y el vínculo personal). Se reconoce especialmente cuando se solicita para hacer una acción por responsabilidad médica (ponderación con el **derecho de acceso a la justicia**).

Ver Sentencias T-650/99, T-834/06, T-158A/08, T-303/08, T-837/08, T-1146/08, T-044/09.

Tipo de persona: **figura pública**

El criterio prevalente para decidir casos de "figuras públicas" es la **existencia de un interés público preponderante** y el **asentimiento voluntaria** (del tratamiento) que implica naturalmente una posición pública. Se reconoce que las figuras públicas requieren una protección especial de la honra, para ellos la jurisprudencia considera que los daños morales deben ser incrementados proporcionalmente.

Brasil [21 Junio 2006] **[Tribunal de Justiça do Estado de São Paulo]** Luiz Inácio Lula da Silva vs. Francisco Amaral

Tratando-se de figuras públicas, políticos conhecidos, como o próprio apelante, maior a repercussão da acusação. Assim, também evidente o prejuízo à imagem e honra pessoal do apelado, caracterizando dano moral passível de indenização.

En igual sentido **Brasil** [20 Octubre 2009] **[Tribunal de Justiça do Estado de São Paulo - 15ª Vara Cível]** **Rubens Barricello vs. Google do Brasil**

Este fallo puede ser interpretado que si la indemnización es mayor, de daño es mayor por la misma condición de figura pública.

Mexico [17 Junio 2009] **[Suprema Corte - Primera Sala]** **Tesis: 1a. CCXIX/2009** (ponderación con la libertad de expresión y sustento en el interés público)

Quienes desempeñan, han desempeñado o desean desempeñar responsabilidades públicas tienen pretensiones en términos de intimidad y respeto al honor con menos resistencia

normativa general que los ciudadanos ordinarios (incluye el concepto de umbral de protección del honor e implícitamente a los candidatos)

El subrayado "desean" solo aparece en la jurisprudencia mejicana y es relevante al discutir la publicidad de los padrones electorales (militancia política).

Argentina [Corte Suprema] *Ponzetti de Balbín, Indalia v. Editorial Atlántida S.A.* : la condición de figura pública no se extiende a los familiares.

Según la jurisprudencia de California, EE.UU. existen personas "voluntariamente públicas" y personas "involuntariamente públicas", estas últimas son los familiares de las personas públicas. También establece que la condición de persona pública es por vida y no en función del periodo de exposición pública.

> **Doctrina:** Gary Williams ¿Protege el Derecho Constitucional a la Privacidad en California a las Figuras Públicas de la Publicación de Información Confidencial Personal?
>
> Rodolfo Diego Veljanovich, Análisis del fallo de la Corte Suprema de Justicia de la Nación "Ponzetti de Balbín, Indalia v. Editorial Atlántida S.A.", del 11 de Diciembre de 1984 (Fallos, 306-1892)

Costa Rica [13 Enero 2004] **[Corte Suprema - Sala Constitucional] Sentencia 146/2004. Por** detención del hijo de ex Director del Organismo de Investigación Judicial y por la publicidad que se le dio al caso, lo que considera violatorio de su derecho al honor. Lo interpone contra el OIJ. **Sin lugar.**

"… , la Sala concluye que la información difundida por los medios de prensa, no lesiona el derecho a la imagen del recurrente, por cuanto únicamente se estableció el vínculo filial por tratarse de su hijo, quien fue detenido, y en virtud de que el promovente ocupó un alto cargo público, como el de Director del OIJ. Por otra parte, fue el mismo recurrente, quien decidió brindar declaraciones y facilitar entrevistas a la prensa, tanto escrita como televisiva, otorgando de esta forma su consentimiento para que su nombre e imagen, fueran utilizados por los medios informativos en distintas oportunidades. De conformidad con lo expuesto, no considera esta Sala que con los elementos probatorios que constan en autos se pueda tener por constatada vulneración alguna de los derechos del promovente, ni de los derechos del amparado. En consecuencia, lo procedente es desestimar el presente recurso como en efecto se hace."

> **Doctrina**: María Macarita Elizondo Galperín, Las personas políticamente expuesta y el blindaje de las elecciones
>
> Andréa Neves Gonzaga Marques, Direito à intimidade e privacidade

Legislación:

> **Argentina** [26 Octubre 1999] Ley 25.188 de Ética en el Ejercicio de la Función Pública. ARTICULO 4º — Las personas referidas en artículo 5º de la presente ley, deberán presentar una declaración jurada patrimonial integral dentro de los treinta días hábiles desde la asunción de sus cargos. ARTICULO 6º — La

declaración jurada deberá contener una nómina detallada de todos los bienes, propios del declarante, propios de su cónyuge, los que integren la sociedad conyugal, los del conviviente, los que integren en su caso la sociedad de hecho y los de sus hijos menores, en el país o en el extranjero. ARTICULO 10. — El listado de las declaraciones juradas de las personas señaladas en el artículo 5º deberá ser publicado en el plazo de noventa días en el Boletín Oficial. En cualquier tiempo toda persona podrá consultar y obtener copia de las declaraciones juradas presentadas con la debida intervención del organismo que las haya registrado y depositado,

Resolución por las que se Expiden las Disposiciones de Carácter General a que se Refiere el artículo 95 bis de la Ley General de Organizaciones y Actividades Auxiliares de Crédito Aplicables a los Denominados Transmisores de Dinero por Dicho Ordenamiento". Dicha Resolución en su Capítulo I, denominado Objeto y Funciones, en la fracción novena de su base segunda, señala que: Para los efectos de las presentes disposiciones se entenderá por:
…
IX . "Persona políticamente expuesta" aquel individuo que desempeña o ha desempeñado funciones públicas destacadas en un país extranjero o en territorio nacional, considerando entre otros, a los jefes de estado o de gobierno, líderes políticos, funcionarios gubernamentales, judiciales o militares de alta jerarquía, altos ejecutivos de empresas estatales, o funcionarios o miembros importantes de partidos políticos Agrega la resolución que para los efectos de la misma "se asimila a las personas políticamente expuestas, el cónyuge y las personas con las que mantenga parentesco por consanguinidad o afinidad hasta el segundo grado, así como las sociedades en las que la persona políticamente expuesta mantenga vínculos patrimoniales"

Tipo de persona: **niños y adolescentes**

Ponderación de derechos: en general se da prevalencia a los Derechos del Niño (excepto con la libertad de expresión). Se menciona reiteradamente en las sentencias el **interés superior del niño**. El acceso a las historias crediticias de menores de edad puede encuadrarse en el criterio de **autonomía progresiva.**

Ponderado con la libertad de expresión

Contrariamente a 535 U.S. 234 (2002) *Free Speech Coalition v. Ashcroft* en **Colombia** la Corte Constitucional menciona que "los menores cuentan con un amparo reforzado". En otras sentencias se menciona el "interés superior del niño" como argumento para este plus (*e.g.* casos de **Costa Rica** y **Chile** sobre imágenes).

Colombia [23 Julio 2009] **[Corte Constitucional - Sala Quinta de Revisión]** **T-105/10** En caso de conflicto entre el derecho a la información o a la libertad de expresión, y el derecho a la intimidad u otro derecho fundamental de los menores, **estos últimos tienen primacía**. Ello no supone prohibir el desarrollo de la libertad de expresión, sino que estrictamente regula su ejercicio para que no se acceda a la intimidad de los menores sin control. En reiterada jurisprudencia[*], la Corte se ha pronunciado sobre la necesidad de garantizar de manera

efectiva y prevalente, el ejercicio de los derechos a quienes por su infancia son sujetos de especial protección. Así se ha estimado que los menores cuentan con un amparo reforzado también cuando se encuentran involucrados en un episodio que podría afectar su derecho a la intimidad, su integridad moral y su formación. No cabe duda que el Estado debe brindar protección prevaleciente a los derechos fundamentales de los niños, inclusive frente a la libertad de informar y ser informado.

El gobierno de los EE.UU. argumentó que la pornografía infantil virtual alimenta el apetito de los pedófilos y los anima a envolverse en conductas ilegales. Este argumento no no fue aceptado por en el razonamiento de los jueces:

> "El gobierno no puede prohibir un contenido por el hecho de que incrementa las probabilidades de que se cometa un acto ilegal 'en algún momento futuro e indefinido' *Hess* v. *Indiana,* 414 U.S. 105, 108 (1973) *(per curiam)*. El gobierno puede suprimir un contenido que abogue por el uso de la fuerza o una violación a la ley solo si 'tal apología está dirigida a incitar o producir una acto ilegal inminente y que probablemente incite o produzca tal acción' *Brandenburg* v. *Ohio,* 395 U.S. 444, 447 (1969) *(per curiam)*. No existe aquí intención, incitación, solicitación, o conspiración. El gobierno no ha mostrado más que una remota conexión entre un contenido que podría animar pensamientos o impulsos que podrían resultar en un niño abusado. Sin una conexión directa y significativamente fuerte, el Gobierno no puede prohibir un contenido sobre la base de que puede animar a los pedófilos a cometer una conducta ilegal."

Una clara señal de la tensión es que a un año de esta sentencia se sanciona la *PROTECT Act* (*Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act*) que establece sanciones penales para la producción, distribución, recepción o posesión de representaciones sexualmente explicitas de un niño, no siendo un elemento requerido que el niño presente en las imágenes realmente exista.[5]

Derecho de intimidad en relación con sus padres

Argentina [16 Agosto 2011] **[Corte Suprema] V.24.XLVII. In re V., D. L.,** se reprende a los padres por publicar fotos y datos íntimos de sus hijos en en diferentes redes sociales de internet

Colombia [27 Junio 1994] **[Corte Constitucional]** Sentencia T-293-94 se le prohíbe a la madre publicar un libro que revela la vida íntima de sus hijas

En [15 Febrero 2011] **[Canada - Quebec] Cinémas Guzzo inc. c. Berthiaume** se condena por una revisión no corporal desproporcionada tomando en consideración las **consecuencias**, pues determinó que la madre tomara conocimiento que su hija menor utilizaba píldoras anticonceptivas

---

[5] 18 USC Section §1466a. La norma incluye expresamente cuando la representación es un *cartoon* y ha generado la misma reacción que la norma anterior. En Brasil la ley 11.829 establece sanciones penales en el caso de imágenes simuladas y existen divergencias sobre su aplicación a los *cartoons*; sin embargo se ha establecido que *cartoons* con escenas explicitas son utilizados por pederastas para aproximarse y preparar sus víctimas (*grooming*)

Imágenes - participación en hechos delictivos

Costa Rica [2010] **[Corte Suprema - Sala Constitucional]** **Sentencia 543/2010** La sentencia analiza los limites en la información capaz de identificar a dos adolescentes en el caso. En el primero se consideraron violatorios: en el reportaje que fue exhibido al público en general, se suministraron una serie de datos que, conjugados, permiten con relativa facilidad realizar una identificación del menor sometido al proceso penal. Así, se hizo una enunciación de los delitos por los cuales se le persigue, información que, en principio, solo debería estar al alcance de las partes (a los 1:03 minutos del vídeo aportado como evidencia), se mostró el momento en que la vivienda del joven era allanada (desde los 0:38 minutos del vídeo aportado), se identificó claramente la vivienda del menor amparado (a los 0:43 minutos del vídeo aportado como evidencia), aparecen imágenes de su detención (a los 1:07 minutos del vídeo aportado) y se mostró, sin distorsión alguna, un tatuaje que el menor tiene en su mano derecha (a los 1:17 minutos del vídeo aportado), todos esos datos, unidos, pueden permitir, como se dijo, la identificación del tutelado.

Para el segundo adolescente se determina que no existe una vulneración a los derechos fundamentales de menor de edad citado, ya que, la noticia únicamente hace referencia a un menor de edad de quince años, que alquilaba una casa en barrio México que utilizaba para la venta de drogas. De ahí que, se rechaza que tal información vulnere o atente en contra de la imagen, intimidad, confidencialidad o privacidad de la persona menor de edad.

Chile [2011] **[Corte Suprema - Tercera Sala]** **Rol N° 9301-2010** se ordena retirar fotos de Facebook que podrían vincular dos adolescentes con el saqueo de un supermercado (se fundamenta en el artículo 40 de la Convención sobre los Derechos del Niño)

En **España** [29 Junio 2005] **[Audiencia Nacional - Sala de lo Contencioso-Administrativo]** **Sentencia de 29-06-2005.** ... recurso contencioso administrativo número 897/2003 interpuesto por la entidad "ENTIDAD A" … contra la resolución del Director de la Agencia de Protección de Datos de 26 de septiembre de2003, por la que se impone a dicha entidad, una sanción de multa de 60.101,21 € … ... la inclusión de los datos del menor en el fichero de morosos, a la vista de las circunstancias concurrentes en el -caso de autos y de la redacción del artículo 29 de la LOPD que no efectúa distinción ni exclusión al respecto, y del contenido del artículo 4 de la Ley Orgánica 1/1996, de 15 de enero, de Protección del Menor, no integra la conducta típica apreciada, lo que conlleva la estimación del recurso interpuesto.

La Resolución PS de 26/9/2003 no está accesible pero es imaginable —y de aquí en adelante es solo especulación— que la AEPD realizó una ponderación de derechos de la que concluyo que los datos del menos tendrían una protección especial. La Audiencia Nacional —como suele ocurrir con muchas decisiones judiciales— rechaza las soluciones jurídicas que crean nuevas normas, y en su resolución anula la sanción con el fundamento que "la redacción del artículo 29 de la LOPD que no efectúa distinción ni exclusión al respecto, y del contenido del artículo 4 de la Ley Orgánica 1/1996, de 15 de enero, de Protección del Menor, no integra la conducta típica apreciada", es decir se vuelca sobre la letra de la ley. En vía de argumentación una eventual ponderación de derechos podría rebatirse argumentando el criterio de la **autonomía progresiva** —quizás aun no muy popular en ese entonces— por el cual los adolescentes al poder contraer obligaciones (progresivamente) también podrían ser incluidos en un registro de

morosos. El argumento —aquí— es puramente especulativo, pero intenta mostrar el riesgo de los procesos de ponderación de derechos frente a la aplicación lateral de la ley.

Interés Superior del Niño

México [22 Septiembre 2006] **[Suprema Corte - Primera Sala]** **Tesis de jurisprudencia 99/2006**

no se viola el derecho a la intimidad genética del presunto padre, atendiendo al **interés superior del menor y a su derecho de conocer su origen biológico y la identidad de sus progenitores** (ponderación)

Tipos de persona: **morales**

Con el mismo argumento que para las personas fallecidas, se excluye de los derechos personalísimos a las personas morales, sin descartar que puedan existir otros derechos que guarden alguna similitud.

La tendencia predominante es que la intimidad y la protección de datos personales son derechos personalísimos, y por tanto no alcanzan a las personas morales.

En **México** [23 Enero 2006] Tesis: XIII.3o.12 A, y [28 Julio 2008] Tesis: 2a. XCIX/2008, el derecho a la protección de los datos personales se refiere únicamente a las personas físicas por estar encausado al respeto de un derecho personalísimo, como es el de la intimidad, del cual derivó aquél. Esto es, en el apuntado supuesto no se actualiza una igualdad jurídica entre las personas físicas y las morales porque ambas están en situaciones de derecho dispares, ya que la protección de datos personales, entre ellos el del patrimonio y su confidencialidad, es una derivación del derecho a la intimidad, del cual únicamente goza el individuo, entendido como la persona humana.

También en **Argentina** [23 Marzo 1990] **Kasdorf S. A. vs. Provincia de Jujuy y otro**

> Voto en disidencia del Dr. Jorge Antonio Bacque: Las personas jurídicas, provistas de subjetividad jurídica, poseen atributos de naturaleza extrapatrimonial (prestigio, crédito comercial, derecho al nombre) los que le son reconocidos para el logro de sus fines específicos, y son valorizados por la comunidad en que se desenvuelven, y su menoscabo genera un daño de características similares a la lesión de los bienes extrapatrimoniales característicos de las personas de existencia visible y que deben ser objeto de tutela aún al margen de la existencia de un perjuicio patrimonial actual y cierto. Fija su monto en 389.000.000 australes.

Curiosamente en los procesos de disociación de sentencias realizados en España, se anonimiza también a las personas morales ver por ejemplo **España** [29 Junio 2005] **[Audiencia Nacional - Sala de lo Contencioso-Administrativo]** **Sentencia de 29-06-2005.** (incluso también a los entes

públicos como un Ayuntamiento).[6] En este caso el balance de derechos se debería inclinar a favor de la publicidad de las actuaciones judiciales. ¿Cuál es el argumento subyacente?

categoría: **tipo de datos**

Datos patrimoniales

Honduras [10 Agosto 2008] **[Instituto de Acceso a la Información Pública]** **Resolución 37-2008**

Que el divulgar públicamente que determinado particular está en posesión de una obra de arte de gran valor histórico y económico , la cual forma parte del Patrimonio Cultural de la Nación, equivaldría a generar un margen considerable de riesgo en términos de que se identifique a dicha obra y a su poseedor , como blanco relativamente fácil para la comisión del delitos de robo o hurto según sea el caso, situación cuya prevención cabe perfectamente bajo el supuesto de reserva establecido por el artículo 17, numeral 2 de la Ley de Transparencia y Acceso a la Información Pública.

La decisión se funda en las consecuencias **consecuencias.** Sin embargo el Registro de la Propiedad en Costa Rica es de acceso público por nombre o cedula de identidad. Esto ha llevado a muchos costarricenses que quieren disminuir sus niveles de riesgo y exposición a la creación de sociedades anónimas para la titularidad de sus bienes. Ver **Costa Rica** [17 Febrero 2009] **[Corte Suprema - Sala Constitucional]** **Sentencia 2578/2009**

Tipo de dato: **ambiente laboral**

Uso del correo electrónico: en este punto existen dos líneas jurisprudenciales bien marcadas:

Línea I.

Criterios predominantes: Marco contractual (y sus límites), continuidad de la relación laboral y preferencia por los derechos del trabajador.

Argentina [Cámara Nacional del Trabajo] Así resolvió que si la empresa no dictó ninguna norma -escrita o verbal- sobre el uso que debían hacer los empleados del correo electrónico, con el agravante de que procedió a despedir al trabajador en forma directa, sin hacerle ninguna advertencia previa sobre el uso particular del correo electrónico, el despido no se ajusta a derecho (CNAT, Sala VII, 27/3/2003, Pereyra, Leandro R. v. Servicios de Almacén Fiscal Zona Franca y Mandatos S.A.).

si la empresa advierte a la trabajadora acerca del uso correcto del e-mail, significa que la propia empleadora estaba en conocimiento de la falta que el dependiente estaba cometiendo, por lo que -en lugar de realizar una auditoría unilateral para enterarse del contenido de los emails protegidos por un "password", e inmediatamente después despedirlo-, debió advertir

[6] Ver por ejemplo: http://juzgadomixtoomercantil2cuenca.blogia.com/temas/sentencias-de-la-a.p.-cuenca-en-recursos-derivados-de-este-juzgado.php

formalmente al trabajador para que cesara en su actitud toda vez que, en los casos de duda, las situaciones deben resolverse en favor de la continuidad del contrato de trabajo (CNAT, Sala X, 23/11/2003, "V.,R.I. v. Vestiditos SA"). La inconducta del trabajador, consistente en navegar por Internet, sin prestar el servicio de soporte técnico contratado por el cliente, no constituye un incumplimiento de entidad suficiente para extinguir el vínculo (CNAT, Sala VIII, 30/6/2004, "Guilhem, Gastón D. v. Netpro S.A.").

Chile [Dirección del Trabajo] [24 de enero de 2002] Dictamen K.2517(166)/2001 ORD.:260/19 ¿es lícito que la empleadora tenga acceso a la correspondencia electrónica de sus trabajadores, en el caso que el dependiente use bienes de propiedad de ésta? … En consecuencia, sobre la base de las disposiciones constitucionales y legales precedentes, cúmpleme manifestar a Ud. que de acuerdo a las facultades con que cuenta el empleador para administrar su empresa, puede regular las condiciones, frecuencia y oportunidad de uso de los correos electrónicos de la empresa, pero en ningún caso podrá tener acceso a la correspondencia electrónica privada enviada y recibida por los trabajadores.

Línea II.

Se distingue el correo corporativo

Brasil [18 Mayo 2005] **[Tribunal Superior do Trabalho]** **TST-RR-613/2000-013-10-00.7**

1. Os sacrossantos direitos do cidadão à privacidade e ao sigilo de correspondência, constitucionalmente assegurados, concernem à comunicação estritamente pessoal, ainda que virtual (-e-mail- particular). Assim, apenas o e-mail pessoal ou particular do empregado, socorrendo-se de provedor próprio, desfruta da proteção constitucional e legal de inviolabilidade.

2. Solução diversa impõe-se em se tratando do chamado -e-mail- corporativo, instrumento de comunicação virtual mediante o qual o empregado louva-se de terminal de computador e de provedor da empresa, bem assim do próprio endereço eletrônico que lhe é disponibilizado igualmente pela empresa. Destina-se este a que nele trafeguem mensagens de cunho estritamente profissional. Em princípio, é de uso corporativo, salvo consentimento do empregador. Ostenta, pois, natureza jurídica equivalente à de uma ferramenta de trabalho proporcionada pelo empregador ao empregado para a consecução do serviço.

3. A estreita e cada vez mais intensa vinculação que passou a existir, de uns tempos a esta parte, entre Internet e/ou correspondência eletrônica e justa causa e/ou crime exige muita parcimônia dos órgãos jurisdicionais na qualificação da ilicitude da prova referente ao desvio de finalidade na utilização dessa tecnologia, tomando-se em conta, inclusive, o princípio da proporcionalidade e, pois, os diversos valores jurídicos tutelados pela lei e pela Constituição Federal. A experiência subministrada ao magistrado pela observação do que ordinariamente acontece revela que, notadamente o -e-mail- corporativo, não raro sofre acentuado desvio de finalidade, mediante a utilização abusiva ou ilegal, de que é exemplo o envio de fotos pornográficas. Constitui, assim, em última análise, expediente pelo qual o empregado pode provocar expressivo prejuízo ao empregador.

4. Se se cuida de -e-mail- corporativo, declaradamente destinado somente para assuntos e matérias afetas ao serviço, o que está em jogo, antes de tudo, é o exercício do direito de propriedade do empregador sobre o computador capaz de acessar à INTERNET e sobre o

próprio provedor. Insta ter presente também a responsabilidade do empregador, perante terceiros, pelos atos de seus empregados em serviço (Código Civil, art. 932, inc. III), bem como que está em xeque o direito à imagem do empregador, igualmente merecedor de tutela constitucional. Sobretudo, imperativo considerar que o empregado, ao receber uma caixa de -e-mail- de seu empregador para uso corporativo, mediante ciência prévia de que nele somente podem transitar mensagens profissionais, não tem razoável expectativa de privacidade quanto a esta, como se vem entendendo no Direito Comparado (EUA e Reino Unido).

5. Pode o empregador monitorar e rastrear a atividade do empregado no ambiente de trabalho, em -e-mail- corporativo, isto é, checar suas mensagens, tanto do ponto de vista formal quanto sob o ângulo material ou de conteúdo. Não é ilícita a prova assim obtida, visando a demonstrar justa causa para a despedida decorrente do envio de material pornográfico a colega de trabalho. Inexistência de afronta ao art. 5º, incisos X, XII e LVI, da Constituição Federal.

Esta sentencia reconociendo que las sanciones administrativas no son confidenciales, sin embargo se afirma que **la divulgación de la información debe hacerse dentro del marco de la finalidad por la que recibida**: **Costa Rica** [05 Julio 2005] **[Corte Suprema - Sala Constitucional]** **Sentencia 08799/2005** Es preciso señalar en primer término que **el desarrollo de procedimientos administrativos disciplinarios es privado y la audiencia que en él se celebra es oral y privada**. Sin embargo una vez concluido el procedimiento y firme el acto final, es un documento que no puede ser calificado como confidencial o secreto como afirma el recurrente, pues se trata de un expediente disciplinario de un funcionario público, cuya información puede ser divulgada a solicitud de la propia administración e incluso por particulares en las condiciones previstas en el ordenamiento jurídico (razones de interés público, como el desempeño eficiente del funcionario público). En el caso de estudio, la Sala observa que se infringió en perjuicio del recurrente uno de los principios que integra el derecho a la autodeterminación informativa, el decorrespondencia entre los fines y el uso del almacenamiento y empleo de la información; pues el Jefe de Seguridad del Tribunal Supremo de Elecciones, adjuntó a la circular 008-SV-2005 de 25 de febrero del 2005, dirigida a todos los oficiales de Seguridad del Tribunal, copia de la resolución de la Secretaría del Tribunal Supremo de Elecciones de las 11:45 horas del 2 de febrero del 2005, que sancionó al recurrente con dos días de suspensión sin goce de salario. **El Jefe de Seguridad tuvo conocimiento de tal resolución en su condición de Jefe inmediato del amparado, sin embargo ello no lo autorizaba a utilizar tal información y divulgarla entre todos los compañeros del amparado**, con ocasión de la emisión de una Circular sobre la forma en que se procedería en el futuro en el control de marcas para mejorar el servicio de seguridad en los puestos externos. **El fin para el cual fueron utilizados dichos datos relativos al amparado es diverso al objeto de su almacenamiento por parte del recurrido**, su Jefe inmediato y le ha causado daño psicológico y ha deteriorado su salud, pues según el dicho del amparado sus compañeros han reaccionado en su contra, se han alejado de él. Por todo lo anterior, estima este Tribunal que el recurso debe ser declarado con lugar por la infracción de los derechos tutelados en el artículo 24 de la Constitución Política. De conformidad con lo dispuesto en el numeral 63 de la Ley de la Jurisdicción Constitucional, y al haberse consumado el agravio en perjuicio del recurrente, lo procedente es prevenir al recurrido que no debe incurrir en acto similar al que dio lugar a declarar con lugar el recurso.

Tipo de dato: **electoral**

El criterio predominante en las decisiones en materia electoral es el de **asentimiento voluntario** (a la publicidad y el tratamiento) y también el interés público predominante.

Las decisiones para hacer públicos los datos de los padrones electorales (y en particular la afiliación a un determinado partido político) se fundan en el criterio del **asentimiento voluntario**. De alguna manera hay cierta similitud con la línea jurisprudencia de "figuras públicas" y se podría llegar a inferir que en las decisiones judiciales de México se asimila "militante" a "pre-figura pública" (véase el uso de concepto "pretenden ser" en las Tesis que definen "figuras públicas")

Ver **Mexico** [17 Junio 2009] **[Suprema Corte - Primera Sala]** **Tesis: 1a. CCXIX/2009** la expresión "Quienes …. desean desempeñar responsabilidades públicas" que transformaría a los militantes en pre-figuras públicas.

Igualmente en **Argentina** [14 Abril 2005] **[Cámara Nacional Electoral]** **Susana T. Sánchez Morteo, coapoderada del Partido Nacionalista Constitucional**

Criterio histórico: Costa Rica hace público en Internet su padrón electoral y es descargable, los historiadores explican que la trasparencia se debe a razones históricas en particular la guerra civil por fraude electoral de 1948.[7]

Tipo de dato: **historial crediticio**

La jurisprudencia sobre los datos crediticios es probablemente la **más prolífica** y la que más ha variado y cambiado sus valoraciones en el tiempo, y también la que más atención académica ha recibido; precisamente por la instalación de la necesidad de información que tiene el sistema financiero para poder asegurar a sus depositantes la calidad del crédito que conceden — dato que fue constituyéndose progresivamente en un interés público predominante.

Hacer aquí un análisis completo de este tipo de dato seria hipertrófico, se presenta entonces en análisis de la evolución jurisprudencial en Colombia y algunos ejemplos de otros países (se insistirá más adelante que el criterio predominante ha sido económico y se ha buscado una fundamentación jurídica *ex post*)

[7] El 8 de febrero de 1948 se realizaron las elecciones. Se enfrentan por la Presidencia de la República Rafael Angel Calderón Guardia, por el partido Republicano, con el apoyo de los comunistas, y Otilio Ulate Blanco, representante de la Oposición Nacional, que incluía partidarios de su propio grupo, el Partido Unión Nacional, del grupo figuerista, del "cortesista" y del Partido Social Demócrata. Según el cómputo de votos, el Partido de Ulate resultó triunfador en la elección presidencial (no así en la de diputados). El 28 de febrero el Tribunal Electoral declaró provisionalmente electo a Ulate como Presidente de la República (con el voto salvado de uno de sus miembros), pero el 1º de marzo, ante una solicitud del Dr. Calderón, el Congreso (de mayoría calderonista) anuló el resultado de la votación, acusándola de fraudulenta. Entre los argumentos que se presentaron para defender la nulidad están las irregularidades cometidas con las cédulas de identidad, el hecho de que el **padrón electoral** estaba incompleto, y el incendio de algunas papeletas electorales.

En realidad los fraudes electorales no eran nuevos en Costa Rica. Se practicaban desde mucho tiempo atrás, pero esta coyuntura fue la chispa que desató la tormenta, y fue el motivo inmediato para iniciar la guerra civil, aunque el movimiento armado se venía preparando desde años atrás.

Según el análisis realizado por [2006] **Diego E. López Medina,** **El derecho de los jueces** Legis, Bogotá, 2006, … el cambio de línea jurisprudencial se describe en la siguiente tabla:

¿Bajo qué condiciones específicas puede una base de datos financiera poseer y divulgar información, sobre un deudor sin violar las garantías constitucionales de intimidad y buen nombre?

Amplia protección de la intimidad del deudor	T-414/92 *M. P. Angarita* T-022/93 *M. P. Angarita*	SU-528/93 *M. P. Hernández*	SU-082/95 SU-089/95 T-592/20-03 *M. P. Tafur* T-94/2004 *M. P. Córdoba*	Prevalencia de los intereses a información por parte del sector financiero; el deudor es protegido, no por la garantía de intimidad, sino por la construcción de "buen nombre"

México [30 Abril 2008] **[Suprema Corte - Segunda Sala]** **Tesis: 2a. LXX/2008** Las garantías individuales encuentran sus límites en la Constitución Política de los Estados Unidos Mexicanos de modo directo y de manera indirecta o mediata en la legislación ordinaria, por la necesidad de preservar otros derechos o bienes protegidos constitucionalmente. De acuerdo con ello, si bien el secreto financiero o bancario está protegido por la garantía de seguridad jurídica contenida en el artículo 16, primer párrafo, de la Carta Magna, en su vertiente de **derecho a la privacidad o intimidad, se encuentra delimitado por la protección que debe darse a otros bienes o derechos constitucionalmente resguardados, como es el de los bancos o instituciones de crédito, de los usuarios o de las sociedades de información, a tener conocimiento del historial crediticio de sus clientes o deudores a fin de realizar las operaciones propias de su objeto**.

México [30 Abril 2008] **[Suprema Corte - Segunda Sala]** **Tesis: 2a. LXIV/2008** el secreto financiero o bancario … al estar referido a la historia crediticia de aquéllos, puede considerarse como una extensión del derecho fundamental a la vida privada de la persona, familia, domicilio, papeles o posesiones de los gobernados, protegido por el artículo 16, primer párrafo, constitucional.

Colombia [28 Octubre 2010] **[Corte Constitucional - Sala Novena de Revisión] Sentencia T-847/10** Los administradores informáticos deben obtener autorización previa y expresa de los titulares del dato financiero que se pretende recopilar, tratar o divulgar. Y de la misma manera, deben permitir las solicitudes de rectificación y actualización por parte de los titulares

de los mismos. Si la fuente de la información no logra demostrar o no tiene los soportes del crédito en mora como acontece en este asunto, la obligación ha de concluirse inexistente o, a lo sumo, como una obligación natural ante la imposibilidad de obtener el recaudo forzoso, lo cual deja en entredicho la veracidad de los datos entregados a los operadores de la información.

Caducidad

Colombia [14 Diciembre 2005] **[Corte Constitucional - Sala Septima de Revisión] Sentencia T-1319/05** En lo relativo al manejo de la información, la protección del derecho al buen nombre se circunscribe a que dicha información sea cierta y veraz, esto es, que los datos contenidos en ella no sean falsos ni erróneos. Por su parte, la garantía del derecho a la intimidad hace referencia a que la información no toque aspectos que pertenecen al ámbito de privacidad mínimo que tiene la persona y que sólo a ella interesa. Finalmente, el derecho al habeas data salvaguarda lo relacionado con el conocimiento, actualización y rectificación de la información contenida en los mencionados bancos de datos.

Dado que el término de caducidad del dato no puede ser el mismo, para aquel deudor que cancela, en relación con aquel deudor que no ha cancelado, y ante la evidencia del vacío legal mencionado, el juez debe llenarlo acudiendo al razonamiento analógico, que enseña que donde existe la misma razón debe aplicarse la misma disposición, en este caso, la regla general de la prescripción de la acción ordinaria civil y debe señalar que el término de almacenamiento de datos de individuos que no hayan cancelado sus obligaciones financieras será de diez años termino similar al establecido por el Código Civil para la prescripción de la acción ordinaria.

¿Se viola el derecho fundamental del habeas data cuando se reporta a una central de información crediticia la mora en una obligación comercial, el titular de la deuda paga voluntariamente el valor de la mora luego de enterarse de que ha sido reportado, y la central conserva posteriormente la información financiera negativa?

Colombia [04 Junio 2004] **[Corte Constitucional - Sala Tercera de Revisión] Sentencia T-565/04**
BANCO DE DATOS - Mantenimiento del reporte por el tiempo equivalente al doble del período que duró la mora

Colombia [26 Junio 2009] **[Corte Constitucional - Sala Segunda de Revisión] Sentencia T-421/09** CADUCIDAD DEL DATO FINANCIERO Y CREDITICIO - Criterios y reglas fijadas por la Corte Constitucional en la sentencia C-1011/08 Conforme a la Sentencia C-1011 de 2008, la caducidad del dato financiero y crediticio negativo, ante la extinción de la obligación por cualquier modo, no puede exceder cuatro años, contados a partir del momento en el que la obligación se extinga, esto es, desde el momento en el que deje de ser exigible judicialmente. CADUCIDAD DEL DATO NEGATIVO FINANCIERO POR EXTINCIÓN DE LA OBLIGACIÓN - Jueces de tutela carecen de competencia para definir si la obligación se encuentra prescrita. La Sala advierte que el dato negativo que reposa a nombre del demandante no puede permanecer por más tiempo del fijado en la jurisprudencia de este tribunal, esto es, por más de cuatro años contados a partir del momento en el que la obligación se extinga por cualquier modo. Lo contrario, implicaría la vulneración del derecho al Habeas Data del accionante y por tanto, la pertinencia de las acciones judiciales necesarias para amparar el derecho vulnerado. No obstante, observa la Sala que, en el caso que nos ocupa, aciertan los jueces de instancia en

negar el amparo solicitado por el accionante, debido a que estos carecen de competencia para definir si la obligación se encuentra prescrita, y por tanto, si le asiste derecho al accionante. Así, teniendo en cuenta que la caducidad del dato negativo financiero por extinción de la obligación, depende, para este caso, de la prescripción de la misma, debe el actor acudir a las autoridades competentes para que sea fijada la fecha exacta en la que se dio la prescripción de la obligación contraída con CONFENALCO, para así determinar el momento a partir del cual, de acuerdo con los parámetros fijados por la sentencia C-1011 de 2008, el peticionario puede solicitar el retiro del dato negativo que reposa a su nombre.

Predictores de riesgo (*passagem*)

Chile [31 Enero 2011] **[Corte Suprema - Segunda Sala] L.E.L. vs. Equifax Chile S.A.**

La recurrida establece indicadores de riesgo crediticio o predictores (dirigidos e a determinar la probabilidad de cumplimiento de obligaciones financieras de una persona determinada), que en el caso de sus informes se fundan básicamente, en razón de 3 factores principales, a saber: 1) número de protestos que posee la persona y el número de morosidades; 2) la relativa al número de domicilios; y 3) el número de consultas a los RUT por terceros. La actuación de la recurrida ha sido arbitraria e ilegal puesto que con la elaboración y divulgación del ya mencionado "predictor de riesgo", se han violentado las siguientes garantías del recurrente: a) la establecida en el artículo 19 N° 2, inciso 2°, la que se ve conculcada, toda vez que se le priva o dificulta de modo importante, su derecho constitucional de optar a créditos en el sistema financiero y comercial para adquirir bienes y servicios, situación que no puede ser vulnerada merced un acto arbitrario carente de fundamentación objetiva y legal, como lo es el "predictor de riesgo", contenido en el informe DICOM; b) La del artículo 19 N° 4, que asegura a toda persona el respeto y protección de su vida privada mediante la prohibición de realizar actos que le causen descrédito. SE ACOGE la acción cautelar deducida contra "Equifax Chile" (antes DICOM S.A.)

Este tipo de predictores se denomina "***passagem***" en Brasil o "modificación de los habitos de consumo". Las empresas de historiales crediticios no pueden utilizar este tipo de información:

Brasil [25 Agosto 2011] **[Rio Grande do Sul - Tribunal de Justiça - Terceira Turma Recursal Cível] Processo 71002981744 RS** Em se tratando de bloqueio indevido de cartão de crédito tão somente em virtude da mudança dos hábitos de consumo, tenho que a situação não se justifica visto que competia à administradora do cartão diligenciar na averiguação dos fatos e não, simplesmente, bloquear o cartão de crédito do autor durante viagem internacional.

Quantum indenizatório reduzido para adequá-lo aos critérios de proporcionalidade e razoabilidade, notadamente frente à característica lenitiva e dissuasória da medida e ao parâmetro desta Turma em casos análogos.

A modo ilustrativo —muy habitual en las sentencias de la Corte Constitucional colombiana— en esta sentencia se hace una recapitulación didáctica luego del cambio jurisprudencial:

Colombia [07 Julio 2003] **[Corte Constitucional - Sala Octava de Revisión] Sentencia T-592-03**

> La jurisprudencia constitucional, de manera unánime y reiterada, en cumplimiento de la proyección constitucional de la libertad individual en el derecho a la autodeterminación informática, exija de los operadores informáticos obtener un previa, explicita y concreta

autorización de los usuarios del crédito para recopilar, tratar y divulgar informaciones sobre su intimidad económica, la que deberá utilizarse con miras a preservar la estabilidad económica que comporta la sanidad general del crédito.

Autorización previa del titular no comprende su facultad de autodeterminación informática. Sin perjuicio del consentimiento del titular, la autorización para divulgar la propia historia crediticia, en cada caso, i) debe entenderse otorgada por el tiempo que los datos resulten pertinentes para enjuiciar los hábitos de pago y la solvencia patrimonial de sus titulares, y j) sólo puede abarcar datos ciertos sobre obligaciones dinerarias insolutas, líquidas y exigibles. Lo anterior por cuanto los datos vetustos, caducos e inciertos no determinan el nivel real actual de respuesta patrimonial de cada usuario del sistema, y en razón de que es la certeza sobre las obligaciones realmente impagadas la que permite a quien analiza una solicitud de crédito emitir juicios objetivos de cumplimiento. En fin, resulta sin sustento el dato que permanece en el sistema informático por un tiempo superior al duplo de la mora –comprendida ésta -, en que pudo haber incurrido su titular, porque los comportamientos crediticios son esencialmente cambiantes.

Procedimiento y divulgación de datos de usuarios de servicios financieros. Los datos que registran, procesan y divulgan las centrales de riesgo, sobre el comportamiento de los usuarios del sistema financiero, es de interés general, porque el crédito "es un factor fundamental en la vida económica, particularmente en el sistema capitalista (..) y este requiere de la confianza del público para operar normalmente" .Fundamentada la garantía de conocer y hacer conocer los hábitos de pago de los usuarios del crédito en el interés general, que comporta la estabilidad del sistema financiero, surge una primera limitación de dicha garantía en función de los datos que resultan efectivamente evaluables en el señalamiento de políticas individuales de crédito. En este sentido, en la sentencia SU-082 de 1995 esta Corte sostuvo que la información que registran procesan y divulgan las centrales de riesgo debe ser completa, para que pueda ser tenida como veraz, de modo que "[e]n lo atinente a un crédito, por ejemplo, un banco no daría información completa, si se limitara a expresar que el deudor ya no debe nada y ocultara el hecho de que el pago se obtuvo merced a un proceso de ejecución, o que la obligación permaneció en mora por mucho tiempo. Igualmente, no sería completa si no se informara desde qué fecha el cliente está a paz y salvo"

DERECHO AL OLVIDO - Informaciones negativas - **DERECHO AL OLVIDO** - Restablecimiento del buen nombre e intimidad Quien con el cumplimiento de sus obligaciones logra crear un nombre que en el pasado no ostentó, tiene derecho a exigir que su esfuerzo se refleje en la información que se divulga sobre él, planteamiento éste sostenido por diversas Salas de Revisión, al considerar que "las sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia, después de algún tiempo tales personas son titulares de un verdadero derecho al olvido". Pero el derecho al olvido, a fin de restablecer el buen nombre, no es lo único que cuenta en la definición de los límites de permanencia de los datos adversos en los ficheros de datos, también la dignidad del deudor reclama que la valoración de su conducta se realice en consideración a su condición humana, en función de la cual las personas pueden en todo tiempo recuperar su nombre e intimidad por haber enmendado su conducta.

Límite temporal de datos negativos La permanencia sin límites de los datos adversos a los usuarios del crédito en el proceso informático constituye un abuso de la autorización recibida –artículo 95 C.P.-, y no cumple con el presupuesto de informar con responsabilidad social –artículo 20 C.P. amen de que colisiona i) con la facultad del titular de la información de autodeterminarse, mediante la actualización o eliminación de sus datos del proceso, salvaguardando así su intimidad económica y el derecho a su buen nombre, y ii) con la dignidad humana de quien enmienda su comportamiento mejorando sus hábitos de pago –Preámbulo, artículos 1°, 2°, 5°, 13, y 15 C.P. Finalmente, en punto al poder resarcitorio del tiempo, es evidente que el Legislador no permite pactar sumas compensatorias que excedan el doble de la obligación principal, límite éste que permite a la Sala considerar el duplo de la mora, como criterio válido de permanencia de un dato adverso en el proceso informático, acudiendo a los artículos 1601 y 867 de los Códigos Civil y de Comercio, respectivamente. Es decir que, para conjurar la conservación de la información negativa, al titular de ésta le basta la extinción de la obligación que dio lugar a ella, más el acaecimiento de un plazo igual al de la permanencia inicial del dato adverso, contada a partir de la mora. O sea que, en tanto el Legislador regula específicamente el asunto, conforme lo indican las disposiciones antes referidas, al parecer de la Sala, las centrales de riesgo, haciendo uso de la autorización de su titular, podrán, a partir de la mora, procesar y divulgar informaciones sobre obligaciones insolutas, hasta su extinción, tiempo éste al que se podrá agregar hasta

uno más. LEGISLADOR-Necesidad de reglamentar el proceso informático en relación con el dato negativo Dado el vacío legal respecto de la permanencia del dato negativo en las centrales de riesgo, esta Corporación ha venido insistiendo en la necesidad de que el legislador determine de manera general como le corresponde, qué debe entenderse por dato adverso y por cuánto tiempo éste puede permanecer en el proceso informático, habida cuenta que la competencia de esta Corporación al respecto se circunscribe a "ejercer el control de constitucionalidad sobre la ley que reglamente este derecho (..)"

CADUCIDAD DEL DATO - Límite temporal por pago voluntario

PROCESO INFORMATICO - Igualdad de usuarios de la actividad económica. En punto a la regulación del proceso informático, lo constituye el **derecho a la igualdad de los usuarios de la actividad económica**, dado que el legislador no puede establecer condiciones disímiles en los procesos informáticos, que además de conculcar la igualdad de los agentes económicos produzca distorsiones en el mercado, a menos que derechos de mayor entidad constitucional que las libertades negociales y de empresa lo exijan.

PRINCIPIO DE LA BUENA FE - Relaciones económicas entre entidades de crédito y sus clientes Las entidades de crédito y sus clientes se encuentran vinculados por relaciones económicas fundadas en el postulado de la buena fe y en el deber de respetar los derechos ajenos y no abusar de los propios, conforme lo ordenan los artículos 83 y 95 de la Carta Política. Debe entenderse, entonces, que las personas que entablan relaciones de crédito y simultáneamente autorizan develar aspectos de su intimidad, que incluso pueden perjudicarlas, confían en que su acreedor divulgará la información sólo cuando las circunstancias efectivamente lo justifiquen, y en que sus facultades de intervenir en la recolección, tratamiento y circulación de los datos serán respetadas en las diversas etapas del proceso informático, de manera que sus actividades económicas no sufrirán tropiezos por la divulgación sorpresiva de datos adversos.

PROCESO INFORMATICO - Información del acreedor al usuario sobre divulgación de datos. Así el usuario de servicios financieros predisponga que terceros sean informados sobre su situación patrimonial y hábitos de pago, el receptor de la autorización está en el deber de informarle cómo, ante quien, desde cuándo y por cuánto tiempo su autorización será utilizada, porque una aquiescencia genérica no subsume el total contenido de la autodeterminación informática, prevista en la Carta Política para que a los asociados les sea respetada su facultad de intervenir activamente y sin restricciones, durante las diversas etapas del proceso informático. En consecuencia el acreedor abusa de la previa autorización, impelida por él y así mismo otorgada por su deudor, cuando, fundado en aquella, divulga datos específicos sin enterar a su titular debidamente, así crea contar para el efecto con la aquiescencia sin límites del afectado, porque el postulado de la buena fe obliga a las partes a atemperar los desequilibrios contractuales, en todas las etapas de la negociación.

ENTIDAD FINANCIERA - Límites a la libertad de escoger al usuario del servicio - Circunstancias a tener en cuenta para escoger al usuario del servicio Es cierto que las entidades financieras deben velar por su solvencia y solidez, de modo que tendrían la proclividad de contratar exclusivamente con quienes demuestren mejor situación patrimonial, mayores garantías de cumplimiento y mejores hábitos de pago, pero dado el carácter público del servicio que prestan les corresponde no descartar los criterios subjetivos en la selección de riesgos, porque son éstos los que les permiten atender las expectativas especificas y los intereses concretos de los usuarios del servicio que están llamados a prestar. En este sentido la objetiva desigualdad que existe entre quien demanda un servicio financiero y quien está en capacidad de prestarlo, impone al Estado el deber de exigir de las instituciones de crédito, en todos los casos, pero en especial cuando pretenden fundar la prestación del servicio en las informaciones divulgadas por las centrales de riesgo i) permitirle al interesado exponer las circunstancias que dieron lugar a los registros, ii) considerar la información adicional suministrada por el proponente, y ii) exponer minuciosamente su decisión de no asignar el producto, de abstenerse de prestar el servicio ofrecido, o de prestarlo en condiciones determinadas, a fin de satisfacer las expectativas que el carácter público de la actividad bancaria genera en los usuarios, y las creadas por ella misma, con la presentación individual de sus productos y servicios.

CENTRAL DE RIESGOS - Datos negativos no constituyen sanción. La información atinente a la atención de sus obligaciones por parte de los usuarios del crédito, registrada en las centrales de riesgo, no constituye una sanción, sino una herramienta que dicho sector

requiere para evaluar las condiciones del crédito, partiendo del conocimiento real del riesgo que el solicitante podría representar para el prestamista, conforme a sus hábitos de pago.

ENTIDAD FINANCIERA - Diferencia entre listas negras y listas de riesgos. A propósito del registro de datos negativos en los ficheros de datos, se consideró pertinente distinguir estos reportes, elaborados con el concurso de las entidades financieras, de las **"listas negras"**, porque el ingreso a éstas comporta, en la práctica, "un cierre de la oportunidad del crédito en cualquier establecimiento comercial y financiero", en tanto las **"listas de riesgo"** reportan "el comportamiento histórico del deudor", con el propósito de someterlo al estudio y posterior análisis de la entidad crediticia.

ENTIDAD FINANCIERA - Autonomía contractual - SECTOR BANCARIO - Límites a la autonomía de la voluntad negocial - DEMOCRATIZACIÓN DEL CRÉDITO DE VIVIENDA. Expuso la Corte la **necesidad de democratizar el crédito**, a fin de que la adquisición de vivienda pueda estar al alcance de todas las personas, inclusive de aquellas de menores recursos, por ello indicó que debían rechazarse las practicadas tendientes a obstaculizar el legítimo acceso de las personas al crédito de vivienda, y al cumplimiento de sus obligaciones atinentes al mismo.

DERECHO A LA INTIMIDAD Y AL BUEN NOMBRE - Vulneración por divulgarse datos negativos de los accionantes sin habérseles notificado. DERECHO A LA INFORMACIÓN - Divulgación de datos negativos de los accionantes, sin habérseles notificado Las centrales de riesgo que administran Computec S.A. y la Asociación Bancaria, estuvieron prestas a cumplir el encargo de sus afiliadas de registrar los datos adversos a sus clientes y hacerlos circular, pero no se cercioraron del conocimiento de los afectados, y tampoco les hicieron conocer el proceso que emprenderían, a fin de que éstos pudieran intervenir efectivamente, y desde un comienzo en el mismo, como lo disponen las normas superiores en cita. De ahí que los datos personales de los accionantes, no podrán seguir siendo reportados, hasta tanto sus titulares i) sean debidamente notificados, y ii) se les conceda la oportunidad de ejercer su derecho a la rectificación y actualización.

PROCESO INFORMÁTICO - Reportes en central de riesgo no dan lugar a exclusión de la actividad económica La jurisprudencia constitucional ha insistido, en que los datos personales que registran las centrales de riesgo no comportan sanciones de ningún tipo para sus titulares, y que por consiguiente tales reportes, con independencia de su sentido, no dan lugar a la exclusión de sus titulares de la actividad económica.

DERECHO A LA AUTODETERMINACIÓN INFORMÁTICA - Respeto Quienes reciben y hacen uso de las autorizaciones que al respecto expiden los usuarios del crédito están obligados: 1. A respetar la autodeterminación informática de los otorgantes, en todas las etapas del proceso i) manteniéndolos al tanto de la utilización de su autorización, y ii) permitiéndoles rectificar y actualizar la información, en especial antes de que llegue a conocimiento de terceros.

También se protege cierta "presunción de cumplimiento" si el motivo de un informe es un proceso judicial: **Colombia** [02 Septiembre 2004] **[Corte Constitucional - Sala Segunda de Revisión]** **Sentencia T-846-04** Una vez analizados los antecedentes de esta acción de tutela, se observa por la Sala de Revisión que el problema jurídico radica en determinar si se vulneran los derechos al buen nombre y de habeas data, por el hecho de reportar una persona a las distintas centrales de riesgo, respecto del **supuesto incumplimiento de una obligación cuya existencia y naturaleza están siendo discutidas en un proceso ordinario**.

En **Costa Rica** en términos generales, la jurisprudencia ha considerado que si la información puesta a disposición proviene de registros públicos y es la necesaria para, por ejemplo, otorgar un crédito, no hay violación del derecho a la intimidad (en este sentido ver sentencias 1999–2563 y 1999–4847). Por el contrario, **cuando la información que consta en la base de datos, proviene de una cuyo acceso es privado (por ejemplo la de la C.C.S.S.), la Sala ha estimado**

necesario contar con el consentimiento de la institución custodiante (sentencia 2000–4147). En la Sentencia 2000–1119 por primera vez se analizó el requisito de la exactitud, con relación a la información que maneja ese tipo de empresas. En ese sentido indicó:

> "V.– No obstante lo anterior, siendo la exactitud uno de los requisitos de la información que las bases de datos pueden guardar de las personas, la falta de elementos suficientes para identificar unívocamente a la persona investigada, puede ocasionarle graves perjuicios. En ese sentido, el artículo 93 de la Ley Orgánica del Tribunal Supremo de Elecciones y del Registro Civil, número 3504, de diez de mayo de mil novecientos setenta y cinco y sus reformas, confiere a la cédula de identidad ese carácter. Por lo anterior, considera este tribunal que las empresas administradoras de datos personales tienen la obligación ineludible de verificar que las informaciones almacenadas a nombre de una persona hayan sido obtenidas de forma tal que no quepa duda acerca de la titularidad del afectado, es decir no basta con la advertencia que plantea la empresa recurrida de indicar al afiliado que corre por su cuenta verificar la titularidad de la persona consultada. En razón de lo que dispone el artículo 140 del Código Procesal Civil, en relación con el 243 de la Ley Orgánica del Poder Judicial, en el sentido de que los abogados y sus asistentes debidamente acreditados tienen acceso a los expedientes judiciales, las empresas encargadas de almacenar datos referentes a procesos jurisdiccionales están en la obligación de verificar la exactitud de los datos que registran, estableciendo con claridad –por medio de una revisión del legajo o de una certificación expedida en el despacho– el nombre completo y número de cédula del demandado, y sólo entonces incluirlo en sus registros. Si el afectado solicita por escrito la exclusión de los datos que a su nombre aparezcan y que sean inexactos por indeterminación de la cédula del deudor, la empresa protectora de crédito debe proceder a verificar la exactitud de las informaciones, en los términos antes dichos, o bien a eliminarlos de su base de datos. Como en la especie las informaciones referentes a los procesos judiciales que aparecen a nombre del amparado no han sido transmitidos ni tampoco se constata que el recurrente haya solicitado a la empresa accionada su corrección o eliminación, procede desestimar la presente acción, como en efecto se hace."

Posteriormente, la Sala en la sentencia número 754-2002 del 25 de enero del 2002 dio un paso adelante en la tutela del derecho a la autodeterminación informativa, variando su criterio en cuanto al concepto resaltado en la cita anterior, que **sujetaba la procedencia de la acción de amparo a que el afectado hubiera formulado sin éxito una expresa solicitud a la empresa que almacena sus datos para que corrigiera o precisara los datos en cuestión**. Este Tribunal señaló en la sentencia 754-2002, que **es la empresa usufructuaria de tal información la que está obligada a mantener en sus registros únicamente datos verdaderos y exactos**, por lo que el sólo hecho de que permanezcan en la base de datos informaciones inexactas constituye una lesión al derecho a la autodeterminación informativa del amparado.

Datos que no se relacionan con el crédito

Costa Rica [21 Mayo 2010] **[Corte Suprema - Sala Constitucional]** **Sentencia 9071/2010** Acusa la recurrente que las empresas privadas recurridas mantienen y distribuyen entre sus clientes, **datos privados sobre su persona y familiares cercanos, como sus padres con los cuales para efectos crediticios no tiene vínculo alguno**. Asegura que no ha autorizado a ninguna entidad ni privada, ni estatal a pedir información crediticia o personal a las empresas recurridas, y mucho menos ha autorizado a las empresas accionadas a que almacenen, compilen y distribuyan su información. Lo anterior, en ejercicio de sus derechos a la intimidad, privacidad, libertad personal, libre autodeterminación informativa. Alega que en las bases de datos de las empresas recurridas **aparece información suya que es independiente de cualquier ámbito crediticio** y peor aún, las recurridas han vendido información suya

totalmente desactualizada. Solicita que se les ordene a las empresas recurridas la suspensión de cualquier acceso ilegítimo e inconstitucional a su información privada, no divulgada y confidencial. Se declara con lugar el recurso, únicamente, contra las empresas Cero Riesgo Información Crediticia Digitalizada Sociedad Anónima y Procesamiento de Datos Datumnet Sociedad Anónima. Se ordena al Presidente con facultades de Apoderado Generalísimo de "Cero Riesgo Información Crediticia Digitalizada Sociedad Anónima", que de inmediato **proceda a eliminar de sus bases de datos la información referente a la dirección física y fotografía de la amparada, y aquellos teléfonos fijos de la tutelada que sean de carácter privado**. Asimismo, se les ordena tanto a los representantes legales de "Procesamiento de Datos Datumnet Sociedad Anónima", **eliminar en forma inmediata los datos de la recurrente que se refieran a consultas en las que haya transcurrido más de cuatro años** desde el momento en que se realizaron. Respecto a las empresas Teletec S.A., Protectora de Crédito Comercial Sociedad Anónima y Transunion Costa Rica TUCR S.A., se declara sin lugar el recurso. Existen votos salvados

En el mismo sentido **Costa Rica** [14 Mayo 2010] **[Corte Suprema - Sala Constitucional]** **Sentencia 8782/2010**

Uso de informes crediticios con fines laborales

Costa Rica [18 Septiembre 2009] **[Corte Suprema - Sala Constitucional]** **Sentencia 14775/2009** Alega el recurrente que estando negociando la incorporación a un nuevo empleo, **el posible patrono le informó que no podía contratarle porque aparecen varias deudas a su nombre en su registro personal** que consta en la base de datos de la empresa Datum. Estima que la empresa recurrida solamente **puede suministrar esa información a entidades bancarias o financieras, por lo que hacer una distribución general a cualquier persona o empresa lesiona los derechos de los trabajadores** que no han tenido ningún problema de trascendencia penal, al punto que su hoja de antecedentes penales se encuentra limpia. Agrega que la información que consta en la base de datos es con respecto a procesos civiles por deudas contraídas con cooperativas mientras fue empleado público, pero que las mismas no deberían ser consideradas para ser contratado laboralmente. Se declara con lugar el recurso. Se ordena al Presidente de Datum Sociedad Anónima, **eliminar de inmediato de la base de datos que dicha empresa mantiene sobre el amparado, la información sobre su domicilio**. CL

En el mismo sentido Sentencia **17086-08**

Distinción entre historial crediticio personal y como representante de una persona moral

Costa Rica [17 Febrero 2009] **[Corte Suprema - Sala Constitucional]** **Sentencia 2578/2009** INFORMACIÓN CREDITICIA PERSONAL Y DE LA EMPRESA - Alega el recurrente que la Comisión Nacional del Consumidor, solicitó información a la sociedad WWWDATUMNET S.A. sobre los archivos de reporte para protección de riesgos crediticio de una sociedad que él tiene; sin embargo, los archivos de protección de riesgos crediticios suministrados a él a título personal y no a la sociedad, como debía de ser, pues él no está actuando como persona física y otra es él actuando en su condición de apoderado generalísimo sin límite de suma de una

persona jurídica. Indica que su fotografía está incluida en la base de datos de la empresa Datum, sin su consentimiento, razón por la cual estima que se ha violentado su derecho de imagen. Añade que el informe señala procesos judiciales tanto de su persona en su condición personal, así como de la sociedad de la cual es parte, sin embargo reitera que la sociedad WWWDATUMNET, S.A no debía de haber suministrado la información de procesos judiciales o administrativos en su carácter personal. Se declara con lugar el recurso. Se ordena al representante de la WWWDATUMNET S.A. que elimine de sus archivos y en la página de datum.net los siguientes datos del amparado relativos a: juicios civiles que tengan más de cuatro años de fenecidos por cualquier causa, según los términos de esta sentencia, lo mismo que la fotografía y la información referente a los procesos judiciales de las empresas. En los demás extremos se declara sin lugar el recurso. CL

En el mismo sentido **Costa Rica** [23 Enero 2009] **[Corte Suprema - Sala Constitucional]** **Sentencia 910/2009** Alega el recurrente que solicitó una tarjeta de crédito en el Banco de Costa Rica, entidad para la cual trabaja. Que dicha gestión no se concretó porque según la persona que se encarga de esos trámites le informó que todo se debe a una deuda con la Caja Costarricense de Seguro Social (CCSS) y que aparecía como **patrono moroso** por esa cantidad de dinero. Que en el Banco de Costa Rica que es su patrono, se le limitan las oportunidades para optar por un nuevo puesto ya que los cargos requieren en el perfil del empleado que éste debe tener una conducta intachable, y que en este momento, al aparecer en la CCSS como patrono moroso, le perjudica en todos los aspectos, pues su expediente a nivel crediticio se encuentra manchado. Que su honorabilidad y su nombre se ha visto manchado injustamente, por la negligencia de la CCSS que, a sabiendas de que no ha solicitado ni asegurado a ningún trabajador, emite una orden a la empresa DATUM.NET, y otras, para que se le tenga como patrono moroso, algo que es totalmente falso. Se declara con lugar el recurso. Se ordena al, Presidente de la Junta Directiva de la Caja Costarricense de Seguro Social, o a quien ocupe su cargo, disponer lo necesario para que, de inmediato, se suministre al recurrente un documento idóneo para demostrar que carece de deudas con la institución.

Proporcionalidad

Costa Rica [11 Diciembre 2008] **[Corte Suprema - Sala Constitucional]** **Sentencia 18.444/2008** Violación del derecho alegado por la exigencia del recurrido de la suma de cincuenta dólares para reinsertar los datos del amparado en sus bases de datos, de modo que puedan ser accedidos por las entidades financieras, resulta desproporcionada

Haber sido imputado y sobreseído en un proceso penal: (con lugar) Sentencia 4447-08.

Derecho al olvido – caducidad: (con lugar) Sentencia 8324-11.

Eliminar información privada: (con lugar) Sentencias 6843-11, 11973-10 y 1812-06.

Otras sentencias en **Costa Rica** son amparos para aplicación por reiteración de jurisprudencia ya definida, y muestran la necesidad de acceder a la justicia para su aplicación efectiva (la Sala Constitucional es un tribunal de única instancia al que acuden los ciudadanos para reclamar sus derechos constitucionales).

(Sin lugar) Sentencias 14543-11; 10790-11; 7902-11; 7297-11; 6170-11; 5386-11; 5412-11; 5547-11; 21511-10; 18158-10; 15790-10; 5320-10; 6326-08; 4908-08.

(Con lugar) 11177-11; 7937-11; 7937-11; 17915-10; 10629-10; 9418-10; 5396-10; 16014-06; 14775-09; 910-09; 18444-08; 18189-08; 17086-08; 15967-08; 15601-08; 10114-08; 5135-08.

Entre ellas hay una muy relevante. En el caso el actor no probó los hechos, y la Sala declaro sin lugar el recurso (*i.e*. no hay jurisprudencia) pero este caso es una señal muy importante de política pública porque da indicios del "modelo de negocios" que existe detrás de los informes crediticios:

Costa Rica 14543-11. EMPRESA DE VENTA DE DATOS BLOQUEA INFORMACIÓN AL ORDENARLO LA SALA, NO LA ELIMINA. Alega el recurrente que el dieciséis de agosto de dos mil diez, se apersonó ante las oficinas de Datum situadas en el Paseo Colón, y le informó al Representante Legal de dicha empresa que le habían rechazado un crédito por cuanto no se podía acceder su información por estar bloqueada y, que además esta Sala por medio de la resolución 10-2667 ordenó actualizar de manera inmediata la información referente a su persona. Asimismo, que corrigieran los registros que se refieren a consultas en las que hubiese transcurrido más de cuatro años desde el momento en que se realizaron. Alega que el recurrido, le respondió que la Sala no podía obligarlos a suprimir la información que se encuentra en sus bases de datos, por ser información obtenida de entidades públicas y de la misma página del Poder Judicial. Indica que Datum aplica el bloqueo de datos a todo aquel ciudadano que interpone un recurso de amparo contra ellos, por lo que las malas referencias se mantienen en sus bases de datos con efectos a perpetuidad, y pese a que esta Sala les ordena suprimir dichas referencias, las mismas no son eliminadas, sino que son bloqueadas para que la solicitud de crédito sea rechazada por las entidades financieras. Con base en las consideraciones dadas en la sentencia, se declara sin lugar el recurso. **SL**[8]

Tipo de dato: **Internet**

¿Equivale publicar en Internet a una cesión indiscriminada?

En cuanto al derecho de los ciudadanos al acceso a la información, hay que considerar que el derecho ha de ser lógicamente, no sólo para "acceder", sino para "usar" la información pública. Este es el ámbito en **España** de la **Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público:**

"La información generada desde las instancias públicas, con la potencialidad que le otorga el desarrollo de la sociedad de la información, posee un gran interés para las empresas a la hora de operar en sus ámbitos de actuación, contribuir al crecimiento económico y la creación de empleo, y para los ciudadanos como elemento de transparencia y guía para la participación democrática. Recogiendo ambas aspiraciones la Directiva 2003/98/CE, de 17 de noviembre de 2003, del Parlamento Europeo y del Consejo, relativa a la reutilización de la información del sector público, se adoptó con la finalidad de explotar el potencial de información del sector público y superar las barreras de un mercado europeo fragmentado estableciendo unos criterios homogéneos, asentados en condiciones equitativas, proporcionadas y no

[8] El caso figura en el Boletin de Jurisprudencia de la Sala IV, pero aun no esta publicado en el sitio web.

discriminatorias para el tratamiento de la información susceptible de ser reutilizada por personas físicas o jurídicas."

Colombia [05 Septiembre 2002] **[Corte Constitucional - Sala Séptima de Revisión]** **T-729/02** Ante la posibilidad de acceso a múltiples bases de datos personales (publicadas ahora en la Internet), el fortalecimiento del poder informático (caracterizado por su titularidad en ocasiones anónima), y la carencia casi absoluta de controles, **se han incrementado los riesgos de vulneración efectiva** no sólo del derecho a la autodeterminación informática, sino de los demás derechos fundamentales puestos en juego en el ámbito informático: la intimidad, la libertad e incluso la integridad personal. **{consecuencias}**

Buscadores

Los buscadores en Internet (o buscadores externos, e.g. Google y Yahoo) han sido atacados judicialmente en diferentes aspectos.

Argentina [11 Agosto 2010] **[Cámara Nacional Civil - Sala D]** **D. C., V. vs. Yahoo de Argentina SRL y otro, daños y perjuicios** Se rechaza la responsabilidad civil de los buscadores por la indexación de sitios que tienen contenidos violatorios a la imagen e intimidad de los accionantes.

Sin embargo el voto en disidencia del juez de cámara Diego C. Sánchez retoma el concepto de **tratamiento con fines de lucro**:

"Los buscadores -que son también páginas de internet- quedan, en conclusión, alcanzados por dicha prescripción legal; por lo que la búsqueda y facilitación de contenidos que aquéllos operan quedan enmarcadas en el ejercicio de la libertad de información y la libre expresión (…) El mecanismo que utilizan los buscadores requiere, en una primera instancia, de la sistematización y facilitación de la información de la web; esta actividad opera como antecedente de su efecto consecuente, que es la potenciación de la información; es allí donde creemos que se concreta -o termina de concretarsela antijuridicidad de la actividad de los motores de búsqueda: esta última actividad de publicitar los contenidos dañosos -o del lugar donde se hallan los contenidos- es lo que compromete a las empresas de búsqueda en un orden de causalidad dañoso, que se dispara con el proveedor del contenido ofensivo (antecedente) y se potencia (consecuente) con la accesibilidad masiva que posibilitan los buscadores; el daño es, así, causado directamente por el proveedor del contenido ilícito, y potenciado por el divulgador, que se sirve de aquél para **su aprovechamiento económico**.

"Las empresas de búsqueda, en tanto se aprovechan de esa facilitación de contenidos lesivos de derechos de la persona humana, deben responder jurídicamente, no ya por los daños que ocasionan esos terceros proveedores de la información que sistematizan, sino por el carácter de la misma actividad que desarrollan, que al repotenciar a aquéllos ocasionan también daños".

La legislación española permite una decisión que implica verificar los requisitos para la existencia de responsabilidad **España** [13 Mayo 2009] **[Audiencia Provincial de Madrid - Sección 9ª]** **Sentencia 95/2010** El artículo 17 la Ley 34/2002 **exime de responsabilidad a los prestadores de los servicios que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos**, por la información que dirijan a los

destinatarios de sus servicios siempre que se cumplan **determinados requisitos**, como son que no tengan conocimiento efectivo de la ilicitud de la información o que lesiona bienes o derechos de terceros susceptibles de indemnización o bien que teniendo dicho conociendo actúen con diligencia para suprimir o inutilizar el enlace correspondiente, estableciendo dicho precepto que un prestador de servicios tiene conocimiento efectivo a los efectos de dicha exención de responsabilidad cuando un órgano competente haya declarado la ilicitud de los datos, ordenando su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, precepto que es consecuencia de la transposición del artículo 13 de la Directiva 31/2000.

En un caso análogo **España** [17 Septiembre 2008] **[Audiencia Provincial de Barcelona - Sección 15] Recurso 749/2007 Aleix P. L., vs. Google Spain S.A.** se rechaza que Google haya infringido, al prestar su "servicio caché" respecto de la pagina web del actor, **los derechos de propiedad intelectual** del actor respecto de su obra contenida en dicha pagina Web, sin que el mero hecho de prestar ese servicio caché constituya una infracción del derecho de reproducción y de comunicación.

Tanta inmunidad se corresponde con la necesidad de que los internautas cuenten con un servicio de indexación en la web, situación que pone a los buscadores dominantes en una posición muy cercana a un servicio público (o *state actors* en la legislación de EE.UU.). Sin embargo recientes críticas han advertido que los buscadores personalizan las búsquedas según los datos históricos de quien consulta, bloqueando y privilegiando cierta información —al mismo tiempo los algoritmos de búsqueda e indexación son secretos.

Muchos sitios de gobierno que publican exhaustivamente en Internet —como los sitios judiciales plagados de datos sensibles— han introducido los ***kaptcha*** para excluir a los robots y dar algún tipo de protección mínima a los datos personales (también se recomienda el *Standard de Exclusión de Robots*).

acceso a aplicaciones de e-gobierno por nombre y apellido: ver **Colombia** [05 Septiembre 2002] [Sala Séptima de Revisión de la Corte Constitucional] Sentencia T-729/02

Tipo de dato: **Judicial**

El criterio que se aplica en la ponderación de derechos, en particular la libertad de expresión (y su derivado el derecho de audiencia), y el de publicidad de las actuaciones judiciales (reconocido en la el artículo 8.5 de la Convención Americana sobre Derechos Humanos) que son ponderados con el derecho de autodeterminación informativa, el de presunción de inocencia y los derechos del niño. De esta ponderación surgen tres líneas. En la primera se da preeminencia a la libertad de expresión, en la segunda se decide la ponderación según el tipo de persona o las consecuencias del tratamiento, y en la tercera línea la ponderación se inclina hacia la protección de los datos personales. Las razones de porque existen tres ponderaciones diferentes radica en causas históricas, culturales o de integridad del sistema normativo. También la inserción de la jurisprudencia de cada país en la jurisprudencia internacional tiene

una gran gravitación. Por ejemplo la jurisprudencia de los EE.UU. otorga una preeminencia especial a la liberad de expresión, que ha sido ponderada como preponderante incluso con los derechos del niño.

La decisión de la Suprema Corte de los Estados Unidos en 535 U.S. 234 (2002) *Free Speech Coalition v. Ashcroft* permite inferir de alguna forma un estándar para establecer el balance que debería existir entre la libertad de expresión y los derechos del niño, en el sentido que no es suficiente una mera chance de generar un riesgo sino que sería necesaria —por ejemplo— una conexión directa y significativamente fuerte entre una aplicación dirigida a facilitar la libertad de expresión y un riesgo para los niños y adolescentes.

> "**El gobierno no puede prohibir un contenido por el hecho de que incrementa las probabilidades de que se cometa un acto ilegal** 'en algún momento futuro e indefinido' *Hess* v. *Indiana,* 414 U.S. 105, 108 (1973) *(per curiam)*. El gobierno puede suprimir un contenido que abogue por el uso de la fuerza o una violación a la ley solo si 'tal apología está dirigida a incitar o producir una acto ilegal inminente y que probablemente incite o produzca tal acción' *Brandenburg* v. *Ohio,* 395 U.S. 444, 447 (1969) *(per curiam)*. No existe aquí intención, incitación, solicitación, o conspiración. El gobierno no ha mostrado más que una remota conexión entre un contenido que podría animar pensamientos o impulsos que podrían resultar en un niño abusado. Sin una conexión directa y significativamente fuerte, el Gobierno no puede prohibir un contenido sobre la base de que puede animar a los pedófilos a cometer una conducta ilegal."

Sobre este mismo argumento, este fallo descalifica el criterio de las "consecuencias probables del tratamiento". Véase que de alguna forma este criterio está presente en la decisión de Costa Rica

> Sentencia 15421-2008 del 14 de Octubre: "La inclusión de sentencias penales en páginas *web* es, en efecto, una consecuencia de la publicidad del proceso penal, la cual constituye una garantía fundamental en esta materia, así reconocida en la el artículo 8.5 de la Convención Americana sobre Derechos Humanos. Además, responde al principio de transparencia de las actuaciones públicas y, en particular, de las judiciales pero, lo que es más importante, en el presente caso, es que esa incorporación de las sentencias no resulta contraria al derecho a la autodeterminación informativa. La Sala ha desarrollado ese contenido ampliamente y ha considerado violatorio de esos derechos fundamentales la incorporación de antecedentes penales en bases de datos privadas, accesibles al público, lo que no ocurre en el presente caso. La sentencia es un hecho histórico, cierto; la información es veraz, por cuanto se transcribe el texto literal de la sentencia y su publicación respondo a las exigencias constitucionales desarrolladas por la Sala."

Es en este punto donde los jueces aducen al argumento de "integridad del sistema normativo" pues aceptan que los datos se publiquen en Internet y sean de libre disposición, pero entiende prohibido su tratamiento por parte de particulares. Esto obedece a un concepto de *law enforcement* que en los EE.UU. es capaz de sancionar severamente a quienes intenten un tratamiento de datos "prohibido", asi en Costa Rica unos pocos casos en los que se identifica tratamientos de datos al margen de la ley son sancionados con daños y perjuicios (mientras

que en los EE.UU. serian sancionados con daños punitivos). Un aspecto que esta interpretación obvia, es la existencia de un mercado negro de datos personales, que quizás si este presente en las jurisprudencias que dan preeminencia a el derecho a la protección de datos personales.

Para la información judicial en general existen al menos tres líneas jurisprudenciales:

Línea I. Basadas en las decisiones de **Chile** [03 Julio 2001] ***N. N. c. Corporación Administrativa del Poder Judicial*** y **España** [2006] [Tribunal Constitucional] **Sentencia 114/2006** según las cuales la regla general es la publicación integra de los textos de las sentencias, y la disociación de datos personales ocurre solo de acuerdo a las excepciones de ley. En ambas decisiones se sostiene que que los criterios de publicación son los mismos sean "en soporte papel, electrónico o cualquier otro".

Línea II. En este caso se crean reglas generales para la **publicación disociada** de datos sensibles o confidenciales y se reconoce el derecho de las partes a solicitar la reserva. Se fundamenta en algunas decisiones judiciales y en decisiones administrativas de los tribunales. En **Costa Rica** [2009] **Sentencia 12434-2009** "se ha instruido al personal de la Sala Constitucional sobre las nuevas políticas de la Sala en asuntos de índole confidencial. Se ordena la exclusión del expediente —por ser de índole confidencial— de las páginas de Internet del Poder Judicial".

En **México** [2004] **Reglamento de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal para la aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental** (numerales 1o., 5o., 6o., 7o. y 8o.), reconoce el derecho de las partes mencionadas en el texto integro de la sentencia a su disociación.

México [19 Enero 2005] **[Segundo Tribunal Colegiado en Materia Administrativa - Cuarto Circuito]** **Tesis Aislada: I.4o.A.688 A** los asuntos tramitados ante el Poder Judicial de la Federación constituyen información pública que puede conocerse por cualquier ciudadano sin más restricciones que las que la ley imponga – resulta ineficaz la oposición si **cuando se concluya que de suprimirse tales datos la información cuya publicación se solicita no pudiera conocerse íntegramente o con la transparencia necesaria**. [**ponderación** a favor de publicidad de las actuaciones judiciales].

México [19 Enero 2005] **[Segundo Tribunal Colegiado en Materia Administrativa - Cuarto Circuito]** **Tesis: IV.2o.A.137 A** De los artículos 1o., 5o., 6o., 7o. y 8o. del Reglamento de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal para la aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental; 3o., fracción II y 13, fracción IV, de la ley en cita, se asume que los asuntos del conocimiento de un órgano jurisdiccional del Poder Judicial de la Federación constituyen información pública a la que los ciudadanos deben tener acceso sin más restricciones que las que la ley les imponga; asimismo las partes que en tales asuntos intervengan tienen el **derecho de oponerse a la publicación** de sus datos personales en caso de que se presente una solicitud de acceso a alguna de las resoluciones o a las pruebas y demás constancias que obren en el expediente respectivo, derecho que se les reconoce en la propia ley federal de transparencia y que los órganos jurisdiccionales deben ponderar desde el momento en que se dicta la primera providencia sobre el conocimiento de un asunto. No obstante ello, también de acuerdo con el marco

jurídico aplicable, ese derecho que por principio asiste a todas las partes del juicio, no garantiza que al plantearse la petición deban suprimirse ineludiblemente los datos personales de quien la formula de cualquier documentación que contenga la información a publicar, incluyendo desde luego la sentencia dictada en el asunto. Por el contrario, la recepción de una petición en tal sentido sólo implica que una vez expuesta, el órgano jurisdiccional está compelido a determinar si tal oposición puede surtir efectos, tomando en cuenta si la resolución definitiva del asunto, las pruebas o las demás constancias respecto de las cuales **prevalece el derecho de la sociedad a conocerlas plenamente**, contienen información considerada como reservada en términos de la fracción IV del artículo 13 de la citada ley, lo que implica que el órgano jurisdiccional a cargo del asunto deberá determinar si la información que se solicita sea excluida en caso de publicación, concierne a una persona física, identificada o identificable, o si es la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad; y además si **de publicarse cualquiera de esos datos se puede poner en riesgo la vida, la seguridad o la salud de cualquier persona**, e incluso si la supresión de la información no incide en que la información cuya publicación se solicita no pueda conocerse íntegramente o con la transparencia necesaria, pues de no colmarse esos extremos, el órgano jurisdiccional podrá anticipar que dicha petición es ineficaz y proceder a la publicación de la información correspondiente, con inclusión de aquella que se buscaba fuera suprimida.

En **Brasil** se atiende fundamentalmente al criterio de “consecuencias” el Ato GP N 310/2001 do Tribunal Regional do Trabalho da 24ª. Região

> Dispõe sobre o bloqueio das consultas de processos, por nome das partes, da página na Internet e nos terminais de extrato dos órgãos da Justiça do Trabalho da 24ª. Região.
> O Presidente do Tribunal Regional do Trabalho da 24ª Região, no uso de suas atribuições legais e regimentais,
> CONSIDERANDO que a consulta de processos, por nome das partes, está sendo utilizada como instrumento de discriminação dos trabalhadores que têm ou tiveram ações trabalhista ajuizadas nesta Justiça Laboral;
> CONSIDERANDO que as facilidades oferecidas com a utilização da página na internet e dos terminais de extrato instalados em diversos órgãos da Justiça do Trabalho da 24ª Região tem contribuído para a prática ilegal de discriminação dos trabalhadores que buscam a tutela do Poder Judiciário Trabalhista;
> CONSIDERANDO, ainda, que o direito de ação, garantido pela Constituição Federal, não pode ser objeto de qualquer contrangimento,
> RESOLVE,
> Artigo 1. Determinar o bloqueio da consulta de processos, pelo nome das partes, da página na Internet e nos terminais de extrato dos órgãos da Justiça do Trabalho da 24ª Região.
> Artigo 2. Este Ato entra em vigor na data de sua publicação.
> Artigo 3. Publique-se no Boletim Interno e no Diário Oficial do Estado do Mato Grosso do Sul.
> Campo Grande, 13 de dezembro de 2001
> ANDRÉ LUIS MORAES DE OLIVEIRA
> Juiz-Presidente do TRT da 24ª Região

En **Argentina** [18 Diciembre 2003] **[Río Negro, Superior Tribunal]** **Acordada 112/2003** establece la aplicación obligatoria de las **Reglas de Heredia**

Notas legislativas:

En **Brasil** [2005] **Ley 11.111** se otorga competencia al Poder Judicial para la disociación.

Línea III. Según criterios adoptados todas las sentencias publicadas deberán estar disociadas. Es el caso de **Uruguay** [2006] **Acordada n° 7564**, y **España** por decisión del Consejo General del Poder Judicial.

Asentimiento voluntario: algunos comentarios dicen de un eventual **asentimiento voluntario** para el tratamiento consecuencia del acceso a la justicia. Sin embargo el asentimiento voluntario debe ser consecuencia de una verdadera opción, con alternativas. Ni aun en los procedimientos voluntarios un justiciable concurre como opción a un Tribunal, sino como una necesidad de una decisión o declaración judicial, necesidad que generalmente depende de hechos o acciones que no están en su control ni son parte de sus opciones. En cierta medida los únicos procesos judiciales que derivan de un acto voluntario de la persona concernida, son los que concluyen con una condena penal, situación que es concurrente con la jurisprudencia predominante.

Notas de doctrina:

Eduardo Vázquez Bote, Fulano contra zutano. Un breve comentario sobre la citación jurisprudencial. Revista Crítica de Derecho Inmobiliario. Núm. 511, 1975

Paula Jervis Ortiz, Comentario jurisprudencial. Intimidad y tratamiento de datos personales en el portal del Poder Judicial. Revista Chilena de Derecho Informático. Nº 1, 2002

Tipo de dato: **Judicial,** sub-tipo**: materia penal**

En estos casos suele predominar el interés público que incluye la demanda por seguridad pública, por esa razón la jurisprudencia otorga más trasparencia a los tipos de delitos que afectan a los grupos más vulnerables.

Existe cierta tendencia hacia la publicación de los nombres completos de los condenados, incluyendo el tipo de delito, característica de las víctimas o la reincidencia. Los criterios jurisprudenciales son variados.

En **Argentina** [25 Julio 2005] ***In re Kook Weskott, Matías***, se niega la disociación aduciendo que la publicación de las condenas es parte del reproche social a ciertas conductas.

En **España** [05 Abril 2006] **Sentencia 114/2006 del Tribunal Constitucional** frente a una petición formal del interesado (y aun mediando una absolución) se niega la publicación disociada.

En **Costa Rica** [14 Octubre 2008] **Sentencia 15421-2008**: "La inclusión de sentencias penales en páginas web es, en efecto, una consecuencia de la publicidad del proceso penal, la cual constituye una garantía fundamental en esta materia, así reconocida en la el artículo 8.5 de la Convención Americana sobre Derechos Humanos. Además, responde al principio de transparencia de las actuaciones públicas y, en particular, de las judiciales pero, lo que es más

importante, en el presente caso, es que esa incorporación de las sentencias no resulta contraria al derecho a la autodeterminación informativa." "La sentencia es un hecho histórico, cierto; la información es veraz, por cuanto se transcribe el texto literal de la sentencia y su publicación respondo a las exigencias constitucionales desarrolladas por la Sala."

Sin embargo se considera que estos datos no pueden ser motivo de tratamiento en bases de datos privadas:

Costa Rica [2008] **[Corte Suprema - Sala Costitucional]** **Sentencia 15.421/2008** "La Sala ha desarrollado ese contenido ampliamente y ha considerado violatorio de esos derechos fundamentales la incorporación de antecedentes penales en bases de datos privadas, accesibles al público"

Argentina [2000] Ley 25.326 Artículo 74. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

¿Es ingenuo pensar que una vez que la información esté accesible no entre en el "mercado" y pueda entonces ser utilizada con otras finalidades? Cuando la información es el producto es difícil distinguir entre "mercado" y "mercado negro": si la información se usa para discriminar **{consecuencias}** quien discrimina no necesita "información documental", la discriminación no se fundamenta (un empleador puede recibir un informe telefónico –verbal— que relaciona un candidato a un empleo con un divorcio, una acción legal contra su empleador anterior o incluso vincularlo con un proceso penal o un juicio ejecutivo mercantil). Aun cuando no todas las discriminaciones son injustas, el problema consiste también en que si la información fluye en el mercado negro no hay como defenderse. Además si la información es incompleta es muy fácil hacer una interpretación falsa: estar imputado por un delito no hace a una persona un delincuente, no solo está en juego la presunción de inocencia, está también en juego que los poderes judiciales publican en Internet la imputación pero no publican la conclusión del proceso. Hay quienes predican una apertura de las condenas penales; sin duda es mucho más justo y razonable abrir el acceso a los registros penales, que abrir solo el acceso a las imputaciones y mantener en la opacidad las condenas. La Sala Constitucional de Costa Rica se centra en prohibir el tratamiento de la información (sentencias) que publican en Internet de condenas, y aplica sanciones económicas a las centrales de riesgo que las utilizan, ¿la existencia de un mercado negro es un argumento válido para inhibir o disociar la publicación de condenas —al fin y al cabo toda la información judicial se publica disociada (una sentencia integra es una disociación, un edicto, una notificación también).

Ver: **antecedentes penales, deudores alimentarios, delitos sexuales**

Tipo de dato: **Judicial,** sub-tipo**: materia penal — registros de antecedentes penales**

Antecedentes penales, prohibición del tratamiento en bases privadas

Costa Rica [14 Octubre 2008] **[Corte Suprema - Sala Costitucional]** **Sentencia 15.421/2008** "La Sala ha desarrollado ese contenido ampliamente y ha considerado violatorio de esos derechos fundamentales la incorporación de antecedentes penales en bases de datos privadas, accesibles al público, lo que no ocurre en el presente caso."

Notas legislativas: la publicación y el acceso a los registros de antecedentes penales han tenido cierta apertura, en particular para los delitos sexuales cuando las víctimas son niños o adolescentes. Ver Argentina [Mendoza] y Argentina [Neuquén], Chile, Colombia, México [Nuevo León].

ver: **Argentina** [28 Junio 2006] **[Neuquén]** Ley del Registro de Identificación de Personas Condenadas por Delitos contra la Integridad Sexual. La Ley 2.520 que crea el RIPeCoDIS establece que deberán registrase las huellas dactilares, fotografías, historial criminal, cicatrices, señales, tatuajes, grupo sanguíneo, registro de ADN, domicilio, ocupación y cualquier otro dato identificador de las personas condenadas por los delitos tipificados en el Libro Segundo, título III, capítulos II, III y IV del Código Penal.

Argentina [09 Junio 2004] **[Mendoza]** Ley de creación del Registro de Defensa de la Integridad Sexual

Perú - La Ley Nº 7.222 que crea el REDIS, un sistema de identificación genética de violadores y la publicación de sus fotografías por Internet, todavía no puede entrar en vigor por la falta de normas complementarias.

Chile [10 Septiembre 2004] **Ley 19.970 que crea el Sistema Nacional de Registros de ADN** ... Artículo 4. Registros. El Sistema estará integrado por el Registro de Condenados, el Registro de Imputados, el Registro de Evidencias y Antecedentes, el Registro de Víctimas y el Registro de Desaparecidos y sus Familiares.

En Chile el artículo 7 de la Ley 19.927 introduce modificaciones en el Decreto Ley N° 645 de 1925 sobre el Registro Nacional de Condenas: "Toda institución pública o privada que por la naturaleza de su objeto requiera contratar a una persona determinada para algún empleo, cargo, oficio o profesión que involucre una relación directa y habitual con menores de edad, podrá solicitar que se le informe, para fines particulares, si ésta se encuentra afecta a la inhabilitación establecida en el artículo 39 bis del Código Penal. La misma información podrá ser entregada a cualquier persona que cuente con una autorización expresa de aquel cuyos antecedentes se solicitan, para los fines señalados en el inciso anterior."

ver **Francia**, criterios para la anotación de antecedentes penales (discrecionalidad del juez de sentencia)

Costa Rica **1009-03. ANTECEDENTES PENALES EN INTERNET.** Acusa que en páginas de INTERNET existen datos de causas penales pendientes, información que a su juicio no es pública. Se declara con lugar el recurso. En consecuencia, a las empresas recurridas, retirar de las páginas web que manejan sus representadas la información relativa a los procesos penales en los que la amparada figura como imputada y actualizar la información relativa a los juicios civiles que consigna en la base de datos de su representada dentro de los cinco días siguientes a la notificación de esta resolución. **CL**

Costa Rica 1435-03. INFORMACIÓN POLICIAL ES PRIVADA. Fue despedido de su trabajo, con base en información que una empresa privada le dio a su patrono, que consiste en el listado de los juzgamientos de carácter penal que ha tenido, donde se especifica el despacho judicial, la fecha de ingreso, el ofendido, y el delito, entre otras cosas, dichos datos solo pueden ser obtenidos en varios fuentes: Registro de Delincuencia del Archivo Judicial del Poder Judicial, el Archivo Criminal del Organismo de Investigación Judicial, la Sección de Archivo del Registro Judicial (San Pablo de Heredia). Que la información recopilada y guardada en los registros y bases de datos de las dependencias del Poder Judicial mencionadas no es pública, sino privada y confidencial, y de ninguna manera puede ser facilitada al público, sino a ciertos sujetos por razones expresamente contempladas en el ordenamiento jurídico. Que las empresas recurridas no están autorizadas jurídicamente a obtener esa información, por lo que su ilícita obtención y tenencia contraviene el derecho de autodeterminación informativa consagrado en la Constitución Política y tratados internacionales sobre derechos humanos vigentes en nuestro país, y también el mandato expreso de reserva y confidencialidad que ha dispuesto el legislador respecto toda esta información de naturaleza penal.

Costa Rica 11154-04. USO DE REGISTROS PENALES POR LA CENTRALES DE CREDITO. Sobre información que existe en internet, con su fotografía y una sentencia penal de la cual fue absuelto. Se declara parcialmente con lugar el recurso y en consecuencia se ordena al representante legal de la empresa "Aludel Limitada", o a quien ejerza ese cargo, retirar de las páginas web que maneja su representada, la fotografía del actor, así como la información relacionada con el proceso penal en el que el recurrente fue sobreseído. En lo demás, se declara sin lugar el recurso. **CL**

Tipo de dato: **Judicial,** sub-tipo**: materia penal — delitos sexuales**

Otro aspecto relevante a la política criminal es el uso de formas de alerta a la población sobre la identidad de los delincuentes sexuales, que es al mismo tiempo una forma de sanción adicional. Esta estrategia ha tenido un fuerte desarrollo en los EE.UU. con la creación en la esfera municipal, y en algunos casos estatal, de bases de datos de delincuentes sexuales de acceso público. Un ejemplo de una base a nivel estatal es la del Estado de Vermont [ver Registro de Delincuentes Sexuales de Vermont en el que es posible ver la foto del delincuente y su situación respecto al tratamiento], en otros casos se trata de bases de datos municipales que tienen naturalmente un menor impacto preventivo [ver por ejemplo el sistema accesible en Internet desarrollado por el Snohomish County en el estado de Washington: al ingresar un código postal (ZIP code) es posible identificar en un mapa interactivo, la ubicación, los domicilios y fotos de los delincuentes sexuales registrados: Map of Registered Sex Offenders]. El Departamento de Justicia de los EE.UU. ha coordinado la consolidación de los registros estatales y federales, de esta forma existe el registro Dru Sjodin National Sex Offender Public Registry que puede ser consultado en Internet y que tiene cobertura nacional. [El primer registro de delincuentes sexuales fue creado en 1990 en el estado de Washington. El 17 de mayo de 1996 se aprueba la Megan's Law a nivel nacional que obliga a los estados y condados a mantener registros accesibles al público; ver listado

de sitios por estado. El número de delincuentes registrados es de 566.408 (a diferentes fechas de 2006)].

También existe una legislación similar en Canadá: *Christopher's Law* (Sex Offender Registry), 2000 y el tema está en pleno debate en la Comunidad Europea [ver Estudio de legislación comparada n° 133, sobre infracciones sexuales cometidas contra niños y adolescentes].

En Colombia la Ley 679 de 2001 (artículo 15) crea un sistema de información sobre delitos sexuales contra niños, niñas y adolescentes que incluye el registro de sus autores, cómplices, proxenetas, tanto de condenados como de sindicados. En Argentina se han aprobado dos leyes que siguen esta tesitura: en la provincia de Neuquén la Ley del Registro de Identificación de Personas Condenadas por Delitos contra la Integridad Sexual, del 28 de junio de 2006, y en la provincia de Mendoza la Ley de creación del Registro de Defensa de la Integridad Sexual, del 9 de Junio de 2004. En estas leyes el acceso a los registros no son públicos ni la consulta anónima como en los EE.UU. En Chile el artículo 7 de la Ley 19.927 introduce modificaciones en el Decreto Ley N° 645 de 1925 sobre el Registro Nacional de Condenas: "Toda institución pública o privada que por la naturaleza de su objeto requiera contratar a una persona determinada para algún empleo, cargo, oficio o profesión que involucre una relación directa y habitual con menores de edad, podrá solicitar que se le informe, para fines particulares, si ésta se encuentra afecta a la inhabilitación establecida en el artículo 39 bis del Código Penal. La misma información podrá ser entregada a cualquier persona que cuente con una autorización expresa de aquel cuyos antecedentes se solicitan, para los fines señalados en el inciso anterior." De esta forma y salvando los derechos de la persona concernida, el acceso a la información sobre condenas se torna público. En Costa Rica también existe un proyecto de ley sobre esta misma materia (Proyecto 15.348).

En Argentina las leyes de Mendoza y Neuquén no están en aplicación (no se han creado los registros) ye en **Costa Rica** [16 Junio 2005] **[Asamblea Legislativa]** **Creación del registro de delincuencia de personas que han cometido delitos y contravenciones contra menores de edad** … el proyecto de ley fue descartado con dictamen negativo unanime: " ... El Informe Jurídico de Servicios Técnicos realizó observaciones en cuanto a la forma y de fondo. Las objeciones materiales o de fondo señalan posibles roces de constitucionalidad, tanto en derechos fundamentales como en lo referente a la independencia de poderes. ... "

Tipo de dato: **Judicial,** sub-tipo**: datos pre-judiciales**

Para la decisión sobre el tratamiento de datos pre-judiciales se incluye en la ponderación de derechos la presunción de inocencia. Tanto las decisiones en México como en Costa Rica se hace un balance.

México [12 Agosto 2009] **[Suprema Corte]** **Tesis: 1a. CLXXXVIII/2009** "La toma de fotografías a personas que no han sido puestas a disposición del Ministerio Público en calidad de detenidas o presuntas responsables —cuando éste sólo ha ordenado su localización y presentación—

configura un acto de molestia porque menoscaba o restringe derechos de la persona, al hacer uso de su imagen"

México [03 Noviembre 2010] **[Suprema Corte]** **Tesis 1a./J. 93/2010** "se establecen limitaciones al acceso de las "averiguaciones previas" (adicionales a las del art. 16 de la Código Federal de Procedimientos Penales): contra el acuerdo del juez de distrito por el que requiere a las autoridades responsables la totalidad de las constancias de la averiguación previa durante la tramitación del juicio de amparo indirecto procede el recurso de queja previsto en la fracción VI del artículo 95 de la Ley de Amparo, y de proporcionarse dicha información, queda bajo la más estricta discrecionalidad del juzgador la guarda, custodia y difusión de las pruebas aportadas al juicio, acorde con los artículos 80 y 87 del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo."

Ver: acción de inconstitucionalidad 00026/2009-00 en trámite contra el artículo 16 del Código Federal de Procedimientos Penales

Costa Rica 000990-07. FOTOGRAFIA EN ALBUN DE SOSPECHOSOS DEL OIJ. Señala el recurrente que sin saber cómo ni cuándo se incluyó su fotografía en el álbum de sospechosos del Organismo de Investigación de Alajuela, por lo cual se le tiene como un delincuente o sospechoso de haber cometido algún delito o ser investigado. Sobre los alcances del derecho a la intimidad, tutelado en el numeral 24 de la Constitución Política se citan las sentencias 678-91 y 1026-94. En este caso concreto, consta que la causa contra el amparado feneció con una sentencia de sobreseimiento y aún cuando corrigió la actuación impugnada, se provocó una lesión a los derechos del recurrente. **CL**

Costa Rica Sentencias 8745-03, 8744-05. PUBLICACIÓN DEL ROSTRO DEL IMPUTADO. Diario Extra publicó fotografía de sospechoso de homicidio. Oficiales de Seguridad del MSP le descubrieron el rostro. Se declara parcialmente con lugar en cuanto se dirige contra los oficiales del Ministerio de Seguridad Pública. Se ordena a los oficiales de conformidad con el artículo 50 de la Ley de la Jurisdicción Constitucional, no incurrir a futuro en los hechos que dieron mérito a la acogida del amparo. **CL**

Tipo de dato: **Judicial,** sub-tipo**: obligaciones alimentarias**

México [31 Octubre 2003] **[Tercer Tribunal Colegiado - Décimo Circuito]** **Tesis: X.3o.21 C** - Cuando en un juicio de alimentos la parte deudora se excepciona en el sentido de que hay otros deudores que también deben soportar la carga, y para demostrarlo ofrece el informe que la autoridad judicial solicite a los centros de trabajo de éstos a fin de probar que cuentan con recursos para proporcionarlos, no existe violación de garantías por la circunstancia de que el Juez haya solicitado tal información, porque aun cuando aquéllos tengan el derecho a ser protegidos en su privacidad, lo cual forma parte de la intimidad, en tal caso **habrá de privilegiarse otro valor fundamental que es la cuestión de alimentos, valor superior a la privacidad, ya que la subsistencia de una persona es de mayor preponderancia que el derecho a la privacidad** por estar de por medio la vida humana y el acceso a la justicia como garantía protegida por el artículo 14 de la Constitución. {***ponderación***}

En **Guatemala** [27 Septiembre 2000] **[Corte de Constitucionalidad]** **Expediente No. 438-2000** Con el fin de conocer el contenido del convenio celebrado en el juicio de alimentos un tercero solicito certificación de convenio celebrado en juicio, sin perjuicio de auxiliar o no en el futuro a cualquiera de las partes del fenecido juicio. Invocó en su exposición los artículos 171 y 198 de la Ley del Organismo Judicial y citó los artículos 50, 91, 63, 66, 67, 69, 70 y 79 *ibid.* El tribunal resolvió: "no ha lugar en virtud que el presentado no es sujeto procesal dentro del presente proceso". Se confirma la decisión ya que el solicitante no acredita interés legítimo en el asunto que reclama.

Notas legislativas:

> En **Argentina** el nivel de acceso varía según la provincia, en Mendoza es un registro que lleva el Poder Judicial en el que hay que registrarse personalmente y acceden solo los empleadores, en la provincia de Salta es con búsqueda por nombre o número de documento (www.justiciasalta.gov.ar/deudores-alimentarios-poder-judicial-salta.php) es un sistema web publico e irrestricto, al igual que en **Perú** (http://casillas.pj.gob.pe/redamWeb/) con búsqueda, relación y fotografía del deudor.

Tipo de dato: **medios**

En los medios la **ponderación** es casi siempre con la **libertad de expresión**, que entran en conflicto con el **derecho a la imagen** o con la **honra.** Prevalece —en casi todos los casos— la **libertad de expresión** pero la jurisprudencia busca medidas correctivas, como **bloqueos**, **derecho a réplica**, o **indemnizaciones civiles.**

Prevalencia de la libertad de expresión:

España [09 Julio 2009] **[Audiencia Nacional - Sala de lo Contencioso] SAN 3658/2009**
En las ediciones impresas y digital (por Internet) del diario EL MUNDO DEL SIGLO XXI, editado por la entidad UNIDAD EDITORIAL SA, apareció con fecha 11 de marzo de 2007 un artículo titulado "Laura, 29 años, muerta en vida desde el 11-M". - El artículo incluye dos fotos de la sala donde se encuentran hospitalizados los enfermos con daño cerebral irreversible en la Fundación Instituto San José de (.....), así como una foto de un paciente. En las dos fotos correspondientes a la citada sala, aparecen pacientes de difícil identificación tendidos en camas. Los denunciantes señalan en ambas fotos, mediante una flecha, a una persona, indicando que se trata de la hija de los ahora denunciantes. De la tercera fotografía, en la que se aprecia a uno de los pacientes con más proximidad, los denunciantes no indican nada, encontrándose en cualquier caso el paciente con la cara parcialmente girada hacia el lado contrario a la cámara. ... debemos anular la resolución recurrida ordenando la continuación del expediente con el fin de determinar la posible utilización del dato de la imagen sin que dicha utilización tuviera amparo en la normativa sobre protección de datos.

Bloqueos

Argentina [17 Febrero 2010] **[Santa Fe, Cámara de Apelación en lo Civil y Comercial de Rosario]** **N.N. vs. Editorial La Página S.A., habeas data** … cabe ordenar al medio periodístico que adopte los medios técnicos a fin de que la información publicada no pueda ser accesada a través de buscadores externos o internos por el nombre del actor, e insertar en la noticia una aclaración respecto de que se ha determinado, en estos autos, la falsedad de la frase mencionada, porque el acceso al dato a través de buscadores, ya sean internos del diario o externos, en las condiciones consignadas, sigue generando daños a la persona en una entidad tal que no es comparable de ningún modo con los que pudieran ser provocados por efecto de la publicación de la edición impresa.

La tendencia es excluir la responsabilidad penal. Por ejemplo **España** [18 Septiembre 2009] **[Audiencia Provincial de Oviedo - Sección 2]** **Rollo 319/2009** CALUMNIAS e INJURIAS - Pero es más, como bien se indica en la instancia el hecho de que el querellado sea titular del dominio http:/www.elcomentario.tv, en el que se encuentra el foro de opinión en donde se vertió el comentario discutido, no se estima pueda determinar su imputación, pues a diferencia de lo que sucede con los tradicionales medios escritos –para los que resulta de aplicación sin género de duda la **responsabilidad en cascada del artículo 30 del Código Penal**-, en que existe un conocimiento previo por los responsables del medio de comunicación del contenido de lo que será publicado, en la red no resulta posible un filtrado pleno del contenido de los mensajes que se reciben e insertan en la página o los foros que forman parte de ella por lo que puede suceder que sin intervención alguna del responsable ocurra que se utilice la página para verter expresiones que pudieran ser constitutivas de delito; no siendo por ello suficiente, para pregonar una **responsabilidad penal**, la simple administración de la página puesto que ello no supone participación no ya sólo en la confección de las expresiones sino tampoco en su publicidad y conocimiento de terceros.

Los casos de difamación en la sección "**comente esta nota**" de la edición en Internet suelen ser una fuente de conflicto. En España la legislación establece los limites de responsabilidad, en otros países la situación es mas compleha.

Tipo de dato: **salud**

Derecho probatorio - Pruebas periciales y ofrecimiento de pruebas.

México [02 Octubre 2008] **[Segundo Tribunal Colegiado en Materia Civil - Sexto Circuito]** **Tesis: VI.2o.C.638 C** **"**implican la intromisión a los derechos de la personalidad, intimidad, integridad, individualidad y privacidad", y **México** [14 Agosto 2008] **[Tercer Tribunal Colegiado en Materia Civil - Primer Circuito]** **Tesis: I.3o.C.738 C** "el derecho sustantivo que podría resultar afectado con motivo de la práctica de las mismas es el de la inviolabilidad del cuerpo y mente a que tiene derecho todo ser humano" … (consecuencias) " ... podrían poner al descubierto aspectos o características psicológicas que tal vez nada tengan que ver con el objeto de la prueba". Sobre el mismo punto y en distinto sentido **Argentina** [02 Junio 2011] **[Cámara Nacional de Casación Penal]** **N. H., M. y otro, recurso de casación** por ponderación con los Derechos del Niño. También en contra **México** [07 Junio 2007] **[Cuarto Tribunal Colegiado en Materia Civil - Primer Circuito]** **Tesis: I.4o.C.27 K** por ponderación al considerar **"**de mayor densidad la garantía de debido proceso que la privacidad"

Colombia [12 Mayo 2010] **[Corte Constitucional - Sala Plena]** **Sentencia C-334/10** Las muestras biológicas representan para el sujeto de quien se han extraído, ante todo un objeto contentivo de información genética que reposan en laboratorios, consultorios y bancos biológicos y hace parte de la información reservada, sometida a un régimen de protección especial, la cual por su estrecha relación con los derechos fundamentales del titular -dignidad, intimidad, libertad, habeas data y autodeterminación informativa y libertad negocial- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. **De este modo, será el juez de control de garantías, quien deberá propender por la armonización entre la práctica de medidas de investigación y el respeto de los derechos fundamentales.**

Colombia [05 Septiembre 2002] **[Corte Constitucional - Sala Séptima de Revisión] T-729/02** DATOS PERSONALES EN PAGINA DE INTERNET DE SUPERINTENDENCIA NACIONAL DE SALUD - Se violan principios. Considera la Corte que, con la publicación de la base de datos sobre los afiliados al sistema integral de seguridad social en Salud, la Superintendencia Nacional de Salud vulnera el derecho fundamental a la autodeterminación informática del actor. En efecto, toda vez que este tipo de datos personales está catalogado como información semi-privada, es decir que su acceso se encuentra restringido, la posibilidad de su conocimiento por parte de terceros totalmente ajenos al ámbito propio en el cual se obtuvo dicha información, a partir del sencillo requisito de digitar su número de identificación,**desconoce los principios constitucionales de libertad, finalidad, circulación restringida e individualidad propios de la administración de datos personales**. Por lo anterior, resulta procedente conceder la tutela invocada y ordenar a la respectiva entidad que haga cesar la conducta vulneratoria de su derecho, en el sentido de permitir que cualquier persona tenga acceso a información personal sobre el actor.

Idem **Colombia** [05 Septiembre 2002] **[Sala Séptima de Revisión de la Corte Constitucional] Sentencia T-729/02**

Historial clínico

Al igual que el historial crediticio, el del acceso suele desarrollarse legislativamente, por tratarse de conflictos más generalizados y con tipicidades frecuentes.

En **Argentina** la Cámara Nacional Civil aplico una sanción a un Sanatorio privado que no aportó una historia clínica —por un argumento de extravío— en un proceso por responsabilidad médica. Los jueces de alzada asumieron los argumentos de los demandantes y condenaron al Sanatorio por los daños derivados de la presunta mala praxis médica, aduciendo que se trataba en concepto de daño punitivo por la pérdida de la historia clínica. La Corte Suprema anuló la sentencia con el argumento que la ley no permite los daños punitivos.

Tipo de dato: **telecomunicaciones**

Acoso telefónico

El tema está presente en dos casos en Costa Rica:

Costa Rica [29 Julio 2011] **[Corte Suprema - Sala Constitucional]** **Sentencia 009948/2011** El recurrente manifiesta que funcionarios del Departamento de Cobro del Banco Popular y de Desarrollo Comunal acosan diariamente a su familia al efectuar constantes llamadas —dos o tres veces por día— a una línea telefónica propiedad de su padre, con el fin de que se comuniquen con su madre. Reclama que las constantes llamadas ya alteraron la salud de su abuela, con quien los personeros del banco insisten en dejar mensajes. Por tal motivo, en numerosas ocasiones la recurrente ha solicitado por escrito a la entidad bancaria accionada que cese el acoso al que somete a su familia, pero la situación se mantiene. Se declara CON LUGAR el recurso. Se ordena al Coordinador del Proceso de Gestión Cobratoria del Banco Popular y de Desarrollo Comunal, adoptar las medidas necesarias para que en lo sucesivo ese banco se abstenga de incurrir en las conductas que ocasionaron la declaratoria con lugar de este recurso.

Costa Rica [01 Julio 2011] **[Corte Suprema - Sala Constitucional]** **Sentencia 008791/2011** Menciona el amparado que los recurridos le llaman a su casa de habitación y a su celular, así como, a otra línea telefónica que se encuentra a su nombre y que no es utilizada por su persona, con la finalidad de cobrar deudas pendientes que tiene; que se comunican que sus hijas que no tienen ninguna relación con el asunto. Se declara con lugar el recurso. En consecuencia se ordena al apoderado judicial del Banco Popular y de Desarrollo Comunal, que tome las medidas necesarias para que se deje de llamar a familiares del recurrente para hacer efectivo el cobro de deudas que le son propias a éste.

En **Argentina** en un caso contra los Supermercados Carrefour (publicado en Jurisprudencia Argentina), el titular de un número telefónico hace un reclamo por daño moral por la invasión de su intimidad. En este caso se trataba de un error involuntario en la impresión del número telefónico del supermercado en los tickets de venta, que motivaba un sinnúmero de llamadas a su domicilio. Se indemnizó el daño moral.

Al igual que en las difamaciones por Internet en **Brasil** [18 Octubre 2010] **[Rio de Janeiro, TJRJ, 1ª Câmara Cível]** **C. M. P. vs. Nextel Telecomunicações Ltda** Caracterizada está a falha na prestação do serviço pela ré ao permitir que qualquer pessoa envie mensagens via internet sem se identificar, não fornecendo aos consumidores submetidos ao serviço denominado "torpedo web" a segurança que dele se espera. Correta a sentença ao condenar a ré no pagamento de danos morais à autora, sendo certo que o conteúdo das mensagens foi direcionado à autora e é capaz de abalar sua honra, uma vez que se refere ao relacionamento amoroso desta. Considerando que a autora suportou muito mais que meros transtornos, tem ela direito a ressarcimento por danos morais, que, consoante precedentes desta Câmara e aos princípios da proporcionalidade e razoabilidade, se encontra bem fixado em quatro mil reais. Honorários advocatícios fixados corretamente. Irretocável a sentença, de modo que, por serem os recursos manifestamente improcedentes, aplica-se a regra do artigo 557 do CPC, negando-se seguimento a ambas as apelações. (responsabilidad por productos defectuosos)

Tipo de dato: **vigilancia**

Los temas motivos de las acciones judiciales son la precariedad legislativa. En primer lugar el plazo en que deben ser destruidas las grabaciones y el ámbito de grabación (público o privado) determina

España [10 Febrero] **[Audiencia Nacional - Sala de lo Contencioso-Administrativo]** **Sentencia de 10-2-2011.** ... la grabación en lugares públicos debe realizarse por las Fuerzas y Cuerpos de Seguridad del Estado en aplicación a lo previsto en la Ley Orgánica 4/1997. Entiende la resolución de la Agencia que está acreditada que la grabación se produce en zonas aledañas a la fachada exterior del centro comercial de la empresa recurrente sito en Málaga lo que solo se justificaría en razones de proporcionalidad (a las que se refieren tanto los artículos 4.1 y 2 dela LOPD como el artículo 4 de la Instrucción 1/2006) ...

... se recogen imágenes captadas por las cámaras exteriores de la fachada de EL CORTE INGLÉS, donde se aprecian los vehículos y las personas que circulan por las vías públicas de las calles que demarcan el edificio. Esta visualización de vehículos y transeúntes no encuentra justificación alguna en la normativa específica y obliga a entender que se trata de un uso excesivo que infringe el principio de proporcionalidad de los datos previsto en el artículo 4.1 de la Ley Orgánica de Protección de Datos.

Portugal [12 Junio 2002] **[Tribunal Constitucional]** **Acórdão 255/02** Declara-se a inconstitucionalidade, com força obrigatória geral, por violação do artigo 165º, nº 1, alínea b), da Constituição, das normas dos nºs 1 e 2 do artigo 12º, do Decreto-Lei nº 231/98, de 22 de Julho, que diz "*(1) As entidades que prestem serviços de segurança privada previstos nas alíneas b) e c) do n.º 1 do artigo 2º podem utilizar equipamentos electrónicos de vigilância e controlo; (2) As gravações de imagem e de som feitas por sociedades de segurança privada ou serviços de autoprotecção, no exercício da sua actividade, através de equipamentos electrónicos de vigilância visam exclusivamente a protecção de pessoas e bens, devendo ser destruídas no prazo de 30 dias, só podendo ser utilizadas nos termos da lei penal.*"

Criterios jurisprudenciales

Criterios generales más frecuentes

Ponderación de derechos

Es el criterio más frecuente y en que predomina en tiempo y forma.

… con la Libertad de expresión:

España [09 Julio 2009] **[Audiencia Nacional - Sala de lo Contencioso]** **SAN 3658/2009**

… con los Derechos del Niño:

Colombia [23 Julio 2009] **[Corte Constitucional - Sala Quinta de Revisión]** **T-105/10**

investigación de paternidad **Mexico** [22 Septiembre 2006] **[Suprema Corte - Primera Sala] Tesis de jurisprudencia 99/2006**

… junto con la dignidad humana:

México [19 Octubre 2009] **[Suprema Corte - Pleno]** **Tesis: P. LXV/2009** … los **derechos personalísimos** deben entenderse como **derechos derivados del reconocimiento al derecho a la dignidad humana**

REVISTA ABUSIVA situações humilhantes e aviltantes da dignidade da pessoa humana: Brasil + Colombia [16 Agosto 2005] **[Corte Constitucional] Sentencia T-848/05**

… con los derechos del niño

Argentina Noble, chile investigación de paternidad, obligaciones alimentarias

… con la seguridad pública

Costa Rica [12 Enero 2010] **[Corte Suprema - Sala Constitucional] Sentencia 543/2010** Queda prohibida la publicación del nombre o cualquier dato personal que permita identificar a una persona menor de edad autora o víctima de un hecho delictivo, salvo autorización judicial fundada en razones de seguridad pública

España [10 Febrero] **[Audiencia Nacional - Sala de lo Contencioso-Administrativo] Sentencia de 10-2-2011.** … la videovigilancia en lugares públicos debe realizarse por las Fuerzas y Cuerpos de Seguridad del Estado

Revista abusiva Colombia [16 Agosto 2005] **[Corte Constitucional] Sentencia T-848/05** no es razonable una requisa que se realice transgrediendo el derecho a la dignidad humana de la persona (reclusa o visitante) al manipular sus partes íntimas, cuando no es necesaria por existir otros mecanismos para garantizar la seguridad.

Interés público predominante (en este caso el interés público puede ser independiente de la voluntad de la persona concernida)

Costa Rica [13 Septiembre 2002] **[Corte Suprema - Sala Constitucional]** **Sentencia 8996/2002** Si la información reviste algún **interés público**, la Sala ha considerado que no es necesario el consentimiento de la persona para utilizar sus datos, lo que solo sería necesario frente a un interés privado. En este sentido, ha manifestado: *Sobre la necesidad de que el interesado dé su expreso consentimiento para la recolección y uso de datos referentes a su persona, esta Sala considera que ello es cierto cuando se trata de datos personales de interés meramente privado. No ocurre lo mismo respecto de la información que revele el historial crediticio de una persona, la cual es necesaria para la protección de una actividad mercantil de interés público y necesaria para el desarrollo, como lo es el crédito. En ese sentido, no resultaría lógico exigir que toda persona diera su expreso asentimiento para el almacenamiento de datos suyos referentes a créditos anteriores, pues posiblemente las personas con problemas de pago estarían renuentes a prestar sus datos, y así el sistema perdería el sentido que tiene. Además, procede esta información de transacciones comerciales realizadas por el recurrente, mismas que no obedecen a una obligación de confidencialidad excepto que exista pacto expreso o que así lo indique la Ley. Por lo anterior, también en cuanto a este aspecto considera la Sala que no lleva razón el petente, por lo que deberá ser desestimado el recurso, como en efecto se hace…*" (sentencia 4749–99 de las 16:27 horas del 22 de junio de 1999).

Orden público e interés social:

México [22 Abril 2009] **[Séptimo Tribunal Colegiado en Materia Administrativa - Primer Circuito] Tesis: I.7o.A.635 A** Los lineamientos mencionados, expedidos por la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, se consideran de **orden público e interés social**, porque su finalidad es otorgar seguridad, primordialmente, al limitar el uso de la información de las personas físicas que no quieren que se utilicen sus datos para fines mercadotécnicos o publicitarios

México [25 Febrero 2005] **[Suprema Corte - Segunda Sala] Tesis: 2a. XXXIV/2005** orden público e interés social (registro público de usuarios -personas físicas- que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios)

… igualdad ante la ley

Chile [06 Octubre 2010] **[Corte de Apelaciones de Temuco - Segunda Sala] N° 1395-2010-PROT** Que la privacidad familiar alegada, no puede ir por sobre el derecho de un probable hijo no matrimonial del causante, a investigar su filiación, lo que atentaría contra el principio de igualdad ante la ley.

La publicidad de los precedentes (o decisiones judiciales) se funda (en la doctrina) en el principio de igualdad ante la ley (no se encontró este argumento en la jurisprudencia analizada)

Proporcionalidad del tratamiento

España [16 Diciembre 1996] **[Tribunal Constitucional] Sentencia 207/1996** "exigencias del principio de proporcionalidad será preciso: a) que **sea idónea (apta, adecuada) para alcanzar el fin constitucionalmente legítimo** perseguido con ella (art. 18 C.E.D.H.), esto es, que sirva objetivamente para determinar los hechos que constituyen el objeto del proceso penal; b) que **sea necesaria o imprescindible** para ello, esto es, que no existan otras medidas menos gravosas que, sin imponer sacrificio alguno de los derechos fundamentales a la integridad física y a la intimidad, o con un menor grado de sacrificio, sean igualmente aptas para conseguir dicho fin; y c) que, aun aun siendo idónea y necesaria, el sacrificio que imponga de tales derechos **no resulte desmedido** en comparación con la gravedad de los hechos y de las sospechas existentes."

Consecuencias probables del tratamiento

Daño innecesario: México [01 Octubre 2009] **[Cuarto Tribunal Colegiado en Materia Administrativa - Primer Circuito] Tesis Aislada: I.4o.A.688 A**

México [15 Junio 2004] **[Séptimo Tribunal Colegiado en Materia Administrativa - Primer Circuito] Tesis: I.7o.A.312 A** los sujetos obligados por dicha norma deberán adoptar las

medidas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, transmisión y acceso no autorizado

Honduras [10 Agosto 2008] **[Instituto de Acceso a la Información Pública]** **Resolución 37-2008** Que el divulgar públicamente que determinado particular está en posesión de una obra de arte de gran valor histórico y económico , la cual forma parte del Patrimonio Cultural de la Nación, equivaldría a generar un margen considerable de riesgo en términos de que se identifique a dicha obra y a su poseedor , como blanco relativamente fácil para la comisión del delitos de robo o hurto

Colombia [05 Septiembre 2002] **[Corte Constitucional - Sala Séptima de Revisión]** **T-729/02** Ante la posibilidad de acceso a múltiples bases de datos personales (publicadas ahora en la Internet), el fortalecimiento del poder informático (caracterizado por su titularidad en ocasiones anónima), y la carencia casi absoluta de controles, **se han incrementado los riesgos de vulneración efectiva** no sólo del derecho a la autodeterminación informática, sino de los demás derechos fundamentales puestos en juego en el ámbito informático: la intimidad, la libertad e incluso la integridad personal.

Brasil [12 Febrero 2009] **[Minas Gerais - Tribunal de Justiça do Estado - 13ª Câmara Cível]** **R. S. B. v. Google do Brasil Internet Ltda.** À medida que a Provedora de Conteúdo disponibiliza na Internet um serviço sem dispositivos de segurança e controle mínimos e, ainda, permite a publicação de material de conteúdo livre, sem sequer identificar o usuário, **deve responsabilizar-se pelo risco oriundo do seu empreendimento**. Em casos tais, a incidência da responsabilidade objetiva decorre da natureza da atividade, bem como do disposto no art. 3º, § 2º, do Código de Defesa do Consumidor. Não tendo o réu apresentado prova suficiente da excludente de sua responsabilidade, exsurge o dever de indenizar pelos danos morais ocasionados. O arbitramento do dano moral deve ser realizado com moderação, em atenção à realidade da vida e às peculiaridades de cada caso, proporcionalmente ao grau de culpa e ao porte econômico das partes. Ademais, não se pode olvidar, consoante parcela da jurisprudência pátria, acolhedora da tese punitiva acerca da responsabilidade civil, da necessidade de desestimular o ofensor a repetir o ato.

Asentimiento voluntario que implica un escrutinio público: el tratamiento consecuencia de un **acto voluntario** de la persona concernida

Aparece en los fundamentos de publicidad de los padrones electorales.

México [07 Octubre 2009] **[Suprema Corte - Primera Sala]** **Tesis: 1a. XLI/2010**

México [17 Junio 2009] **[Suprema Corte - Primera Sala]** **Tesis: 1a. CCXIII/2009** **el comportamiento de sus titulares puede influir en la extensión de su ámbito de protección**. No se trata sólo de que el entendimiento de lo privado cambie de una cultura a otra y que haya variado a lo largo de la historia, sino que **forma parte del derecho a la privacidad**, como lo entendemos ahora, **la posibilidad de que sus titulares modulen, de palabra o de hecho, su alcance**.

Tratamiento con fines de lucro: es utilizado tanto como argumento como por su incidencia en la indemnización por daño moral (como mecanismos indirecto de protección de la intimidad, honra y datos personales)

Brasil [12 Febrero 2009] **[Minas Gerais - Tribunal de Justiça do Estado - 13ª Câmara Cível] R. S. B. v. Google do Brasil Internet Ltda.** " ... à medida que a apelante disponibiliza um serviço sem dispositivos de segurança e controle mínimos e, ainda, permite a publicação de material de conteúdo livre, fomenta a procura pelos usuários, principalmente por aqueles que pretendem praticar atos ilícitos à margem de qualquer controle.

Nessa ótica, levando em consideração que a apelante disponibiliza tais serviços e aufere, com isso, **lucros substanciais**, seria um contra-senso não responsabilizá-la pelo próprio risco do empreendimento.

Nesse ponto, cabe reportar-se às considerações exaradas na sentença: "o anonimato garantido pela demandada lhe é muito conveniente, posto que ao saberem que qualquer pessoa pode fazer qualquer comentário na Internet, seja através de "blogs", seja através de "Orkut", mais e mais internautas acessaram as páginas e sites da ré, **fazendo com que seus lucros aumentassem**. Assim, se opta por não fornecer o nome e IP de quem criou a página, deve arcar com a responsabilidade daí decorrente, não podendo se isentar de culpa"

Argentina [11 Agosto 2010] **[Cámara Nacional Civil - Sala D] D. C., V. vs. Yahoo de Argentina SRL y otro, daños y perjuicios** (voto en disidencia)

Criterios secundarios

Relación de debilidad entre la persona concernida frente a quien hace el tratamiento: es visible en algunas decisiones en ambiente laboral y sobre historial crediticio

Colombia [28 Octubre 2010] [Corte Constitucional - Sala Novena de Revisión] Sentencia T-847/10 … existe una clara relación de *"indefensión"* de la actora como usuaria del sistema financiero frente a la entidad bancaria, porque ante la situación que plantea existe una ausencia o insuficiencia de medios físicos y jurídicos de defensa que le permitan resistir u oponerse a la agresión, amenaza o vulneración de sus derechos fundamentales. De este modo, la entidad bancaria detenta una **posición dominante** frente a la accionante ya que, además de fijar los requisitos, condiciones y registrar la información de los créditos, son las depositarias de la *confianza pública*

Colombia [23 Febrero 2010] [Corte Constitucional - Sala Tercera de Revisión] Sentencia T-129/10

Colombia [16 Octubre 2008] [Corte Constitucional - Sala Plena] Sentencia C-1011/08

Colombia [14 Diciembre 2005] [Corte Constitucional - Sala Séptima de Revisión] Sentencia T-1319/05

Colombia [07 Julio 2003] [Corte Constitucional - Sala Octava de Revisión] Sentencia T-592-03

Criterios históricos: pueden verse en la ponderación a favor de la libertad de expresión en los EE.UU. o a favor de la trasparencia en Costa Rica (de los padrones electorales)

Garantía de audiencia: (en el procedimiento de acceso a los datos personales, documentos e información en posesión de los Poderes de la Unión u órganos constitucionales autónomos o con autonomía legal**:** **México** [09 Septiembre 2005] **[Suprema Corte]** **Tesis: 1a. XXXVI/2006**

Obligación de seguridad: **México** [15 Junio 2004] **[Séptimo Tribunal Colegiado en Materia Administrativa - Primer Circuito]** **Tesis: I.7o.A.312 A**

Criterios de economía social. Tanto en las sentencias de Colombia como Costa Rica se ponderan derechos fundamentales (intimidad) contra interés público definido como la necesidad de los ciudadanos con respecto a un sistema bancario y financiero sostenible. El argumente llama la atención, pues tiende a fortalecer sistemas que buscan predominar (como las exigencias de los bancos o de los buscadores de internet) y que terminan teniendo privilegios o inmunidades. Las sentencias no analizan la existencias de "sistemas" alternativos (e.g. hay otros sistemas como el ahorro, cooperativismo) también incide la incapacidad del sistema de justicia para ejecutar las deudas.

Finalidad: el criterio debería ser más frecuente; aparece en el uso de información crediticia para fines de selección laboral y en otros casos similares

Costa Rica [18 Septiembre 2009] **[Corte Suprema - Sala Constitucional]** **Sentencia 14775/2009** Alega el recurrente que estando negociando la incorporación a un nuevo empleo, **el posible patrono le informó que no podía contratarle porque aparecen varias deudas a su nombre en su registro personal** que consta en la base de datos de la empresa Datum. Estima que la empresa recurrida solamente **puede suministrar esa información a entidades bancarias o financieras, por lo que hacer una distribución general a cualquier persona o empresa lesiona los derechos de los trabajadores** que no han tenido ningún problema de trascendencia penal, al punto que su hoja de antecedentes penales se encuentra limpia. Agrega que la información que consta en la base de datos es con respecto a procesos civiles por deudas contraídas con cooperativas mientras fue empleado público, pero que las mismas no deberían ser consideradas para ser contratado laboralmente. Se declara con lugar el recurso. Se ordena al Presidente de Datum Sociedad Anónima, **eliminar de inmediato de la base de datos que dicha empresa mantiene sobre el amparado, la información sobre su domicilio**. CL

En el mismo sentido **Costa Rica** [15 Febrero 2006] **[Corte Suprema - Sala Constitucional]** **Sentencia 1812/2006** registro de información personal que no tiene que ver con el fin de protección al crédito - La empresa recurrida recolecta, publica y actualiza electrónicamente información personal de los petentes sin haber mediado su consentimiento: **todas las direcciones que han tenido cada uno de ellos, números de teléfonos a su nombre pese a que en el ICE se han pagado como servicios telefónicos privados, fotografías, propiedades y asuntos familiares**.

Responsabilidad civil (daño moral y daño punitivo): muchas sentencias concluyen con la condena por daño moral, como mecanismo implícito de protección de los derechos. La cuantía de los daños es muy baja (en el orden de los 130.000 pesos mexicanos) con la excepción de algunas figuras públicas.

Razonamiento analógico: no se ha encontrado como criterio principal ni secundario

Legalidad: es el criterio residual y por el que los jueces se dividen entre tradicionales e innovadores. En esta materia se debería partir que la ley en débil en sus previsiones casuísticas, y que la decisión judicial debería ser creativa y formular una ponderación. Los jueces temen a la revocación de sus sentencias por aspectos formales o basándose en la letra de la ley.

CONCLUSIONES

En este estudio se ha trabajado con la limitación que el conjunto de sentencias para analizar e inferir criterios era restringido. No obstante se han podido encontrar los criterios más frecuentes y los que se utilizan en forma secundaria. Es posible que existan algunos más en forma residual, y que irán apareciendo en futuros análisis, pero al parecer están reflejados los más importantes.

Si bien no es un objetivo de este estudio, está presente la casuística sobre el tema, que deberá complementarse con la que llega a las autoridades de protección de datos. Esta información es una fuente extraordinaria para los fines regulatorios ya que es la mejor forma de prevención de conflictos.

Se observa que en algunos temas el recurso a la justicia es muy frecuente y reiterado, en particular en historial crediticio (podría ser también imagen, salud, medios, pero en menor medida). Asombra que conflictos similares sigan presentándose, situación que implica un bajo nivel de acatamiento a las reglas jurídicas, probablemente por el hecho que los tribunales no aplican multas, y sus herramienta de disuasión es el daño moral. Muchas decisiones “instan”, “piden” .. o palabras similares el respeto de la lei o la jurisprudencia … que en el modelo de negocios de los datos personales aparece como un mecanismo muy débil de hacer cumplir la ley.

En la medida que la información incluida en este estudio se considere de utilidad se sugiere motivar en el seno de la RedIPD el sostenimiento, continuidad y actualización de la base de jurisprudencia.

ESTUDIO SOBRE EL DESARROLLO JURISPRUDENCIAL EN IBEROAMÉRICA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

reglas de estilo y pertenencia
criterios de sostenimiento de la carga de la jurisprudencia, habilitación de claves de acceso
clasificación por país de la jurisprudencia

1. Reglas de pertenencia

En esta etapa los criterios de pertenencia utilizados fueron:

Sentencias que integran la base de jurisprudencia deben tener las siguientes características:

1.1. Tribunal

Se preferirán las sentencias de los máximos tribunales o autoridades (Cortes Supremas, Tribunales Constitucionales). Las decisiones de otros tribunales inferiores se incluirán con un criterio más restrictivo. En primer lugar las de apelación y residualmente las de primera instancia solo si la solución permite imaginar que esta una nueva línea jurisprudencial en ciernes, o que las condiciones fácticas son relevantes.

En esta etapa no se han incluido sistemáticamente decisiones de otros órganos de impartición de justicia (en particular las agencias nacionales de protección de datos, porque se estimaba que el primer "test" al que se querían someter las decisiones era respecto de su revisión judicial). En próximas ediciones de la base de jurisprudencia si será relevante incluir decisiones jurisdiccionales administrativas pero cuidando seleccionar aquellas que si definan una interpretación o aplicación de la ley realmente novedosa, por su solución o por las condiciones fácticas.

También en un futuro sería conveniente incluir los códigos de autorregulación

Si se incluyen las decisiones supranacionales, en particular los tribunales y comisiones de derechos humanos de América y Europa.

1.2. Criterio de sostenimiento

Para que la Base de Jurisprudencia cumpla una función efectiva, para el IFAI y para la RedIPD debe estar actualizada y completa. Para lograr ambos objetivos es necesario poner en movimiento a las únicas personas capaces de realizar este trabajo: los miembros de la red.

Se sugiere proponer primero a la RedIPD la inclusión de la base de jurisprudencia en una de las reuniones de trabajo, bajo la forma de un Seminario en el que se discuta las categorías propuestas y los criterios utilizados, se deberá buscar una aproximación al consenso y definir reglas escritas.

Luego podría proponerse a cada país que nombre un enlace o corresponsal, encargado de seleccionar los fallos pertinentes y subirlos a la plataforma.

Es conveniente en forma paralela que los miembros asociados a la RedIPD —generalmente académicos— hagan un trabajo de supervisión y control de los contenidos. Muchos países

tenderán a subir sentencias de primera instancia que no contienen ningún criterio jurisprudencial y que son la simple aplicación de la ley por parte de los jueces; harán esto por el solo hecho de querer ver reflejado a su país entre los que inciden en la evolución de la jurisprudencia (por eso las reglas de inclusión deben ser muy claras y restrictivas). También se sumaran muchas decisiones que manejan reglas procesales que no suelen ser relevantes.

Los académicos deben ayudar a mantener coherente la base y equilibrar los contenidos — satisfaciendo las nacionalidades— pero manteniendo la utilidad.

Un recurso de este tipo será usado por quienes deban tomar una decisión y necesiten inspiración y referencias. Pero también podría tener una utilidad como observatorio y fuente de noticias (o temas que están tomando relevancia)

Se recomienda incluir: legislación, documentos de autorregulación y noticias periodísticas. Estos contenidos animan a los interesados a ingresar regularmente al sitio, para mantenerse informados: las noticias y las novedades cumplen una función latente en el decisor que sabe donde tienen recursos para ampliar sus referencias en el momento que las necesite.

Reglas de inclusión

La decisión debe contener un criterio jurisprudencial nuevo en el país, o una variante de una jurisprudencia ya definida. Se excluyen los procesos en los que se aplica lisa y llanamente jurisprudencia anterior (estos casos son comunes en Costa Rica donde la Sala Constitucional es de única instancia y resuelve conflictos entre particulares). Cierta tolerancia podría incluir casos en los que las condiciones fácticas revistan especial interés.

Igualmente podrían ser de interés por alguna disidencia

Cada caso debe ser asignado a la categoría que más se ajusta a la decisión y al criterio jurisprudencial acuñado.

Se sigue el criterio de incluir en el home del país solo las sentencias de los más altos tribunales (de última instancia) o los tribunales internacionales

En el home del sitio se colocaran los anteriores que tengan menos de 6 meses de decididos.

Se ha incluido una categoría para “doctrina” que es muy restrictiva, solo debería utilizarse para escritos que comenten un fallo judicial, o varios, o creen línea jurisprudenciales

2. Reglas de estilo

Cada sentencia se incluye con la siguiente estructura:

Tribunal se coloca entre corchetes describiendo primero la división territorial (si se aplica, solo en países federales), luego el tribunal y finalmente la sala o estructura interna. **Tener cuidado que el texto comience con un corchete y no con un espacio en blanco, en ese caso no asigna el código de colores para el tribunal.**

Argentina [30 Julio 2004] **[Jujuy - Cámara Civil y Comercial]** **S. M.y otro vs. Jujuy Digital**

Sobre la referencia al caso se seguirá el estilo o costumbre predominante en cada país, puede ser el número de sentencia, las partes en el caso, o el número de proceso

Brasil [18 Mayo 2005] **[Tribunal Superior do Trabalho]** **TST-RR-613/2000-013-10-00.7**

Para otras citas que no sean jurisprudencia se puede seguir el criterio:

Doctrina

> **Chile** [2002] **Paula Jervis Ortiz, Comentario jurisprudencial. Intimidad y tratamiento de datos personales en el portal del Poder Judicial** *cache*
>
> Revista Chilena de Derecho Informático. Nº 1, Año 2002

Notas de prensa

> **México** [28 Septiembre 2011] **[nota de prensa en *El Mundo*]** **La directora de un colegio obliga a 20 niños a desnudarse para buscar 13 dólares** *caché*

Fecha

Se incluye la fecha de la decisión (no de su publicación). En algunos casos no se dispone del día o del mes (podrían dejarse en blanco), no se pueden incluir sentencias sin año.

Links

En el campo URL se deberá incluir un enlace externo al texto integro o síntesis de la sentencia. Se dara preferencia a sitios oficiales.

Si el enlace es a una editorial o sitio responsable de jurisprudencia, se podrá colocar solo si no existe enlace oficial

Si el enlace es a un blog o sitio informal o personal, se deberá agregar en la sección del cache [FUENTE NO VERIFICADA]

Resumen o síntesis

Se realizara un resumen breve de la sentencia, en los aspectos más relevantes. En el orden de 10 líneas. El texto podría contener enlaces externos (e.g. a legislación o doctrina, o a otras jurisprudencias)

Cache

Toda la información disponible debe colocarse en el cuadro destinado al cache “con la **finalidad** que sea posible realizar búsquedas en el sitio”. Existe un botón que dice “publicar texto completo” si se activa, aparecerá la palabra cache luego del nombre del caso, y el texto incluido podrá ser visible.

No es necesario formatear el contenido del cache, mas aun un exceso de formato podría evidenciar que se está excediendo la finalidad.

La única razón para incluirlo es la movilidad de los URL profundos en muchos sitios judiciales, que cambian permanentemente.

Uso de idiomas

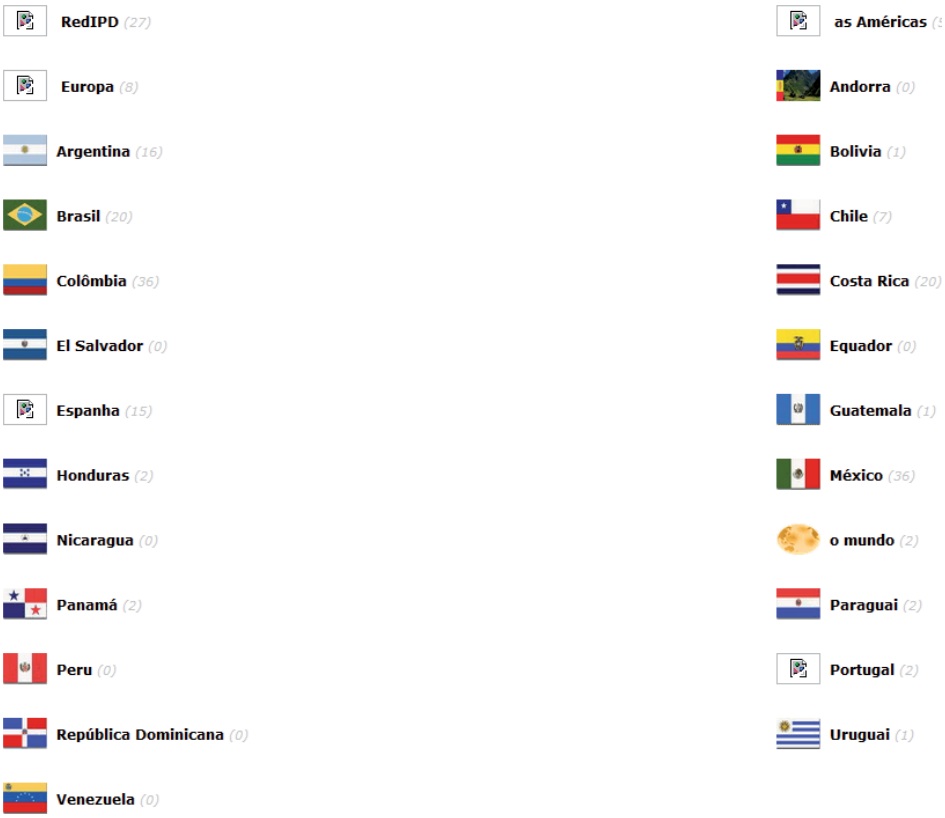
El nombre de los casos siempre respeta el idioma oficial del país, no se traduce a los demás idiomas

Si se dispone de una traducción del resumen puede colocarse en el cuadro correspondiente al idioma.

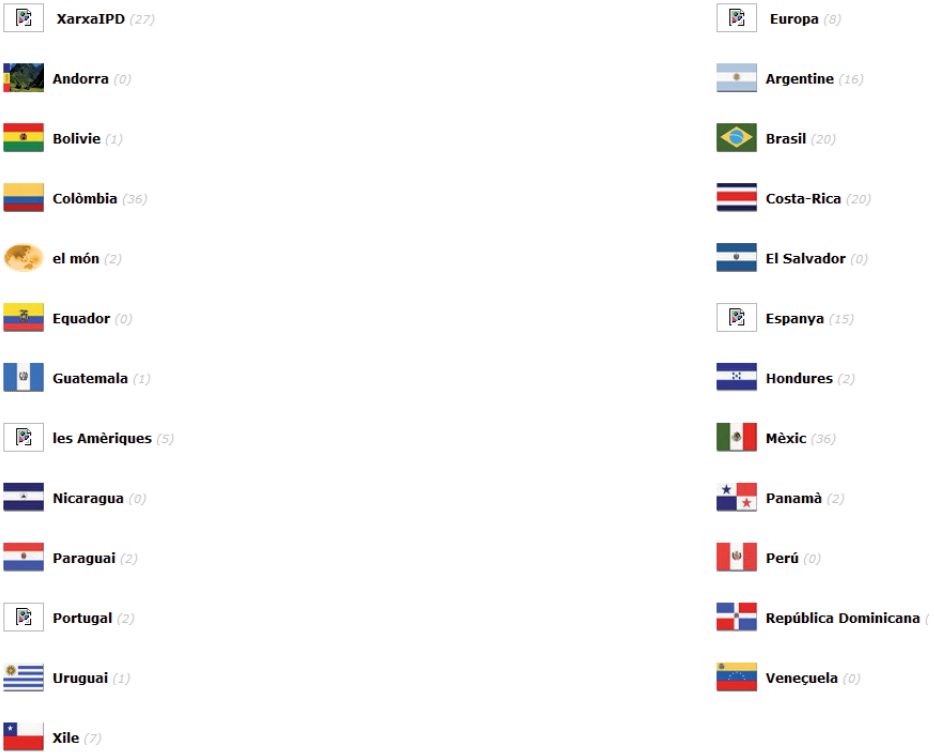
Nota importante: si se está ingresando una sentencia o resumen que no es en español y no se dispone de la traducción al español, el texto en portugués, catalán o ingles deberá colocarse en el espacio reservado para el "español" (o sea que opera como idioma por defecto.

Países

Los países tienen nombres asignados en español, portugués y catalán (el Ingles esta activo pero actualmente no se usa)



En catalán



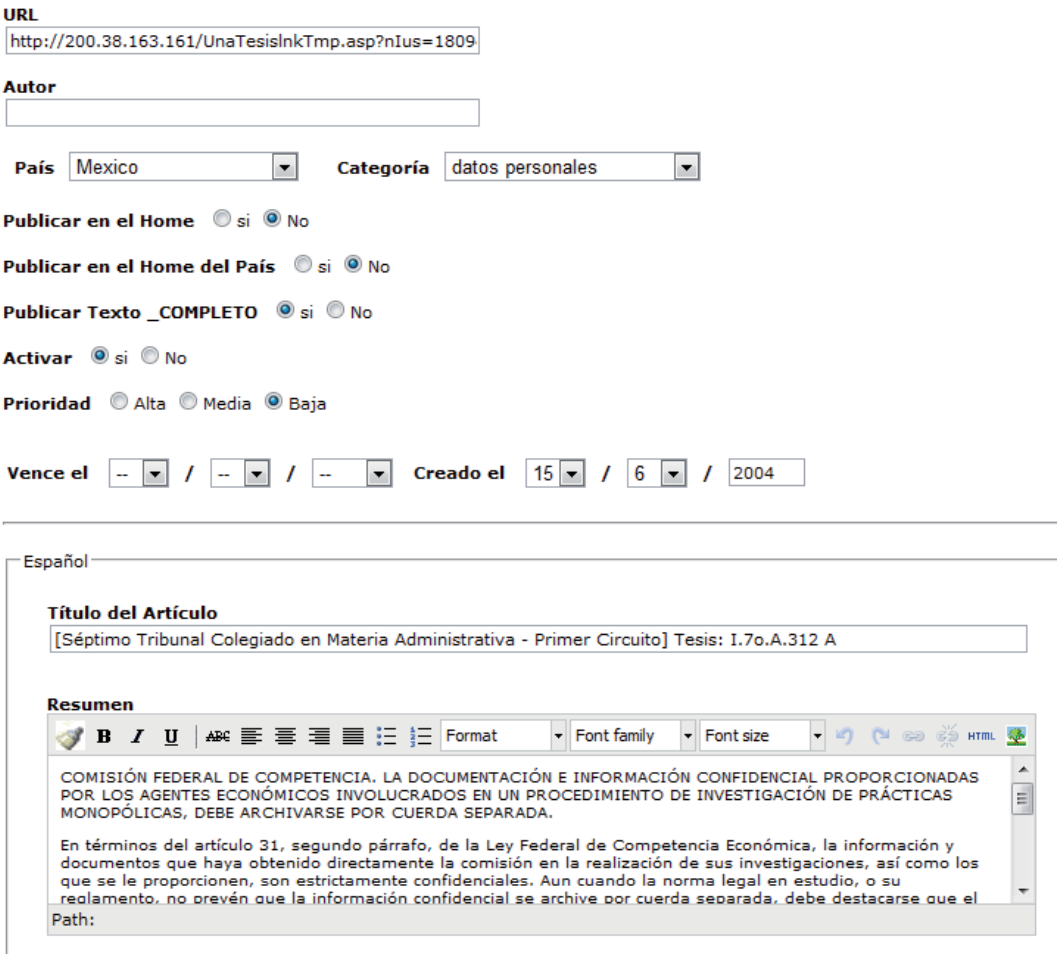
Nota: faltan algunas banderas que deben ser subidas al servidor por el webmaster de www.ifai.org.mx

Criterios adicionales de estilo

Evitar textos en primera persona, uso abusivo de las mayúsculas (se recomienda el uso absolutamente restrictivo). En la práctica es conveniente observar el estilo existente y tratar de continuarlo.

3. Definición de las tareas de sostenimiento

3.1. Carga - Detalles técnicos



El campo “autor” no se utiliza (dejar en blanco)
El campo activar, permite mantener los datos guardados, pero no serán visibles, se utiliza cuando se está trabajando en un caso, pero solo se ha guardado un borrador.

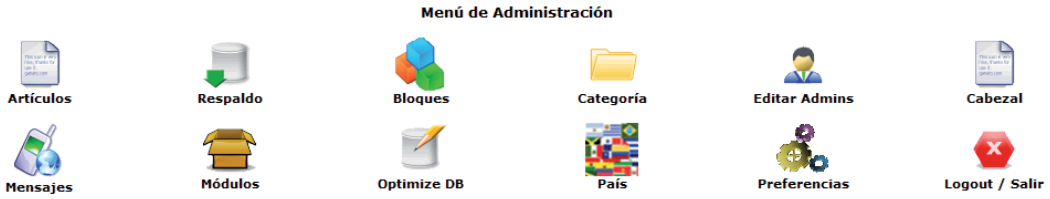
El campo, “vence el” no se utiliza
“creado el” es para la fecha de la sentencia

Prioridad, altera el orden en como aparecen en el home del país, es preferible no asignar prioridades y dejar que se aplique el orden por defecto.

Al concluir se puede apretar cualquiera de los botones que dicen “terminar”.

Panel de administración

En el panel de administración existen otros botones para configurar la presentación, los cabezales de cada categoría, y los pies de página.



Al iniciar la sesión, el botón de artículos es el que habilita la carga.

Respaldo, es un botón para el administrador y hace una back-up de toda la base de datos.

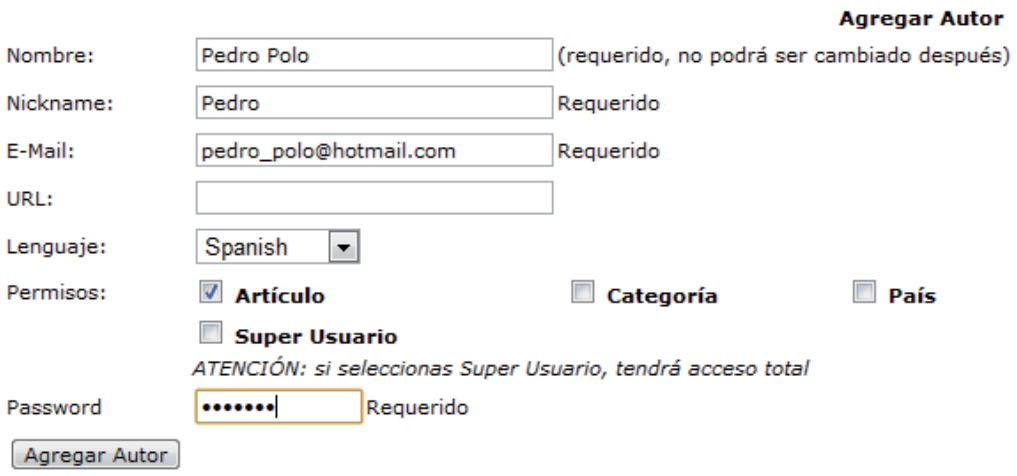
Mensajes, módulos y cabezal, controlan los textos fijos

País, permite quitar o agregar países, lan banderas deben estar alojadas en el servidor para que sean accesibles

Categorías, permite crear o modificar categorías. Cada categoría admite un texto que la describe.

Claves de acceso

La pantalla que crea claves de acceso "editar admins" en el panel principal, permite asignar niveles de usuarios.



La selección para un usuario por país, deberá incluir solo la casilla **Artículo** palometeada. La asignación de control en las categorías y los países no es recomendable, al igual que las cuentas "*god*" que son solo para quien gestiona la base.

Cada autor puede solo modificar los casos (Artículos) que el ingresó.

Instituto Federal de Acceso a la Información y Protección de Datos

DECLARACIÓN DE LA CIUDAD DE MÉXICO

33ª Conferencia Internacional de Comisionados de Privacidad y Protección de Datos

Considerando que la agenda que nos ha convocado a esta 33ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en México pone de manifiesto la naturaleza global tanto del tratamiento de los datos personales como de su protección;

Considerando que el creciente alcance global de las tecnologías de la información, tales como la internet y la telefonía móvil, constituyen un reto y una oportunidad para conformar una comunidad capaz de hacerles frente mediante la elaboración de normas, estándares y metodologías con alcances semejantes al de aquéllas y no obstante las diferencias culturales, la diversidad de actores interesados y sin reparar en los enfoques locales o regionales que se adoptan respecto a la privacidad;

Considerando que el vasto campo institucional de la protección de datos ha evolucionado de sólo un puñado de autoridades a una presencia cada día más global que se expande ahora en América Latina, Asia y África, al tiempo que los marcos normativos de mayor tradición se encuentran actualmente inmersos en procesos de revisión tanto en Europa como en los Estados Unidos de América;

Considerando que a las autoridades de protección de datos y salvaguarda de la privacidad se les exige una protección más efectiva del derecho fundamental a la privacidad en esta nueva era de transformaciones aceleradas;

Reconociendo lo anterior, esta Conferencia ha adoptado una resolución sobre coordinación internacional para la aplicación de medidas protectoras de la privacidad (*Resolution on Privacy Enforcement Coordination at the International Level)*, basada en los fundamentos de la *Iniciativa de Londres*, así como en la Directiva Europea de Protección de Datos y los Acuerdos Asia-Pacífico de Cooperación entre Autoridades de Protección de Datos;

Considerando que las sesiones de la 33ª Conferencia Internacional dejan ver el crecimiento expansivo de las computadoras, los medios de comunicación, el análisis de datos, y la velocidad con la que proliferan los datos personales, así como el desarrollo de nuevas formas de almacenamiento de información en bases de datos de gran dimensión que posibilitan el rastreo y la supervisión, así como las tecnologías basadas en sensores, todo esto comúnmente conocido con el término de "big data";

Considerando que la globalización, los "big data", y la innovación de los servicios en la red, así como los servicios de cómputo en la nube, plantean retos aún mayores para una protección efectiva de los derechos fundamentales;

Considerando que la seguridad de la información personal exige que las organizaciones implementen mecanismos capaces de identificar riesgos para, con un enfoque preventivo poder mitigarlos al tiempo que reaccionar con oportunidad ante una eventualidad;

Considerando que los esquemas de autorregulación, los certificados de privacidad y el principio de responsabilidad representan caminos innovadores susceptibles de ser adoptados por las organizaciones y los profesionales de protección de datos y comprometerse así activamente con la protección de datos;

Reconociendo que los profesionales y expertos de la protección de datos con independencia de que su labor la realicen desde las autoridades, las empresas o las organizaciones de la sociedad civil, dichos empeños serán susceptibles de ampliarse de estar animados por un espíritu de cooperación y colaboración precisado para enfrentar desafíos comunes;

Considerando que los organismos no gubernamentales y la academia a menudo poseen de mayor conocimiento y sofisticación, gracias a las tecnologías de la información de las que disponen;

Los Comisionados del Instituto Federal de Acceso a la Información y Protección de Datos de la Autoridad Anfitriona instan a esta Conferencia a asumir los desafíos que conllevan la protección de datos y la privacidad en una era global, mediante:

1. Comprometerse al diálogo para:
    a. Compartir el conocimiento entre los países, las autoridades y las organizaciones de expertos en materia de privacidad.
    b. Discutir y analizar cómo pueden establecerse prioridades por parte de las autoridades, entidades públicas, empresas y otras organizaciones, para una mejor distribución de los recursos disponibles para la consecución de objetivos comunes.
    c. Explorar la manera en la cual por medio de una transparencia más efectiva, así como por otros mecanismos se puede contribuir a que los individuos comprendan sus derechos y puedan proteger aquellos intereses relacionados con sus datos personales.

2. Impulsar el compartir información con las nuevas autoridades sobre la forma en la cual las organizaciones que emplean datos utilizan las herramientas disponibles para fomentar y promover buenas prácticas en materia de privacidad; así como también la forma en la cual la legislación protectora puede ser aplicada en forma más efectiva, cuando las herramientas para disuadir y alentar resultan ineficientes.

3. Cuidar que el diálogo al que instamos no comprometa la independencia ni socave la efectividad de las autoridades de protección de datos.

4. Acordar que en la 34ª Conferencia Internacional de Comisionados de Privacidad y Protección de Datos se expongan y discutan los avances logrados mediante el trabajo conjunto en aras de una más efectiva protección de datos en esta era de globalización y "big data".

Instituto Federal de Acceso a la Información y Protección de Datos

PRESIDENCIA

"2010, Año de la Patria. Bicentenario del Inicio de la Independencia y Centenario del Inicio de la Revolución".

OFICIO: IFAI/JPM/0108/2010

México, D.F. a 03 de septiembre de 2010

Lic. Eduardo Fernández Sánchez
Director General de Administración
P R E S E N T E

Con la finalidad de dar cumplimiento a lo dispuesto en el Capítulo IV, Artículo 62 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria y Título Segundo, Capítulo Único, Artículo 19, tercer párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, que a la letra dice: "La erogación para la contratación de servicios de consultorías, asesorías, estudios e investigaciones, requerirá de la autorización escrita del titular de la dependencia o entidad, ...",a lo dispuesto en el Artículo Décimo Quinto Fracción II del Decreto que establece las medidas de austeridad y disciplina del gasto de la Administración Pública Federal , que a la letra dice "Se abstendrán de realizar, con cargo al Presupuesto de Egresos de la Federación, la edición e impresión de libros y publicaciones que no sean estrictamente necesarias para el cumplimiento de sus funciones" y a los lineamientos específicos para la aplicación y seguimiento de las medidas de austeridad y disciplina del gasto de la Administración Pública Federal en el numeral 16 y a lo dispuesto en el Capítulo IV, Artículo 63 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, que a la letra dice: "Los titulares de los ejecutores de gasto autorizarán las erogaciones por concepto de gastos de orden social, congresos, convenciones, ...", le informo que se autoriza ejercer las siguientes partidas como a continuación se indica:

Partida 3602 "Impresión y elaboración de material informativo derivado de la operación y administración de las dependencias y entidades."

Unidad Solicitante:	320000 - Dirección General de Clasificación y Datos Personales.
Oficio de Solicitud	IFAI-SA-DGCDP-082-10
Programa:	3. Protección de Datos Personales, Gestión Documental e Indicadores de Gestión.
Motivo:	Considerando que el artículo 38 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, señala que el Instituto tendrá por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana y que México será la sede del VIII Encuentro Iberoamericano de Protección de Datos Personales, se solicita la autorización para ejercer la partida 3602 "Impresión y elaboración de material informativo derivado de la operación y administración de las dependencias y entidades"
Justificación:	El objeto es la impresión de 500 carteles alusivos al VIII Encuentro Iberoamericano de Protección de Datos y 1,500 programas de mano que serán distribuidos entre las organizaciones gremiales, universidades y demás instituciones participantes y entre los participantes al evento los próximos 29 y 30 de septiembre, respectivamente.
Total:	$ 15,000.00 IVA Incluido
Total con letra:	(Quince mil pesos 00/100 M.N.) IVA Incluido

Partida 3701 "Difusión de mensajes sobre programas y actividades gubernamentales"

Unidad Solicitante:	260000 - Dirección General de Comunicación Social.
Oficio de Solicitud	IFAI/SE-DGCS/238/10
Programa:	4. Medios de Comunicación y Difusión.
Motivo:	Se requiere autorización para la realización de un estudio cuantitativo sobre el impacto en la difusión de mensajes de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
Justificación:	Se requiere conocer el alcance e impacto de la difusión de mensajes mediáticos que ha tenido el Instituto así como la percepción que la sociedad tiene sobre la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, así como las funciones propias del IFAI, su nombre como tal y su acrónimo.
Total:	$ 1,000,000.00 IVA Incluido
Total con letra:	(Un millón de pesos 00/100 M.N.) IVA Incluido

Instituto Federal de Acceso a la Información y Protección de Datos

PRESIDENCIA

"2010, Año de la Patria. Bicentenario del Inicio de la Independencia y Centenario del Inicio de la Revolución".

OFICIO: IFAI/JPM/0108/2010

México, D.F. a 03 de septiembre de 2010

Partida 3804 "Congresos y Convenciones"

Unidad Solicitante:	IFAI - Dirección de Recursos Materiales y Servicios Generales
Oficio de Solicitud	IFAI/SE-DGA-drmsg/632/10
Programa:	1. Facilitación y Vinculación
Motivo:	Presentación de la Cartilla Nacional de Derechos y la VII Semana Nacional de Transparencia
Justificación:	En alcance a mi similar IFAI/SE-DGA-drmsg/404/10 de fecha 9 de junio de 2010, se requiere cubrir los costos adicionales que se efectuaron derivado de los eventos que llevo a cabo el Instituto Federal de Acceso a la Información y Protección de Datos, como fueron: la "Presentación de la Cartilla Nacional de Derechos" y la "VII Semana Nacional de Transparencia", en estos eventos se presentó un incremento no previsto de asistentes, el cual conllevo a la ampliación de estructura tecnológica, acondicionamiento del espacio físico, equipo de audio, servicio de coffee break continuo, entre otros.
Total:	$ 256,570.22 IVA Incluido)
Total con letra:	(Doscientos cincuenta y seis mil quinientos setenta pesos 22/100 M.N.) IVA Incluido

Unidad Solicitante:	220000 - Dirección General de Clasificación y Datos Personales
Oficio de Solicitud	IFAI-SA-DGCDP/94-BIS/10
Programa:	1. Facilitación y Vinculación
Motivo:	Se requiere un servicio integral de escenografía, equipo audiovisual y videograbación para el evento "VIII Encuentro Iberoamericano de Protección de Datos Personales" que estará dividido en sesiones matutinas dirigidas al público en general con un aforo aproximado de 800 personas y sesiones vespertinas en las que se desahogaran a puerta cerrada entre los miembros de la Red Iberoamericana de Protección de Datos, cocktel de bienvenida para ponentes y miembros de la Red Iberoamericana de Protección de Datos.
Justificación:	Con motivo del evento a realizarse los próximos 29 y 30 de septiembre, que contará con la presencia de 17 ponentes internacionales, los comisionados del Instituto, representantes de las dependencias reguladoras de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y miembros de los sectores de industrias, comercio y servicios, denominado "VIII Encuentro Iberoamericano de Protección de Datos" dirigido al público en general y en particular a directivos de empresas de sectores deservicio, industria y comercio, se solicita la autorización del ejercicio de presupuesto.
Total:	$ 1,600,000.00 IVA Incluido
Total con letra:	(Un millón seiscientos mil pesos 00/100 M.N.) IVA Incluido

Partida 7502 "Gastos por Servicios de Traslado de Personas"

Unidad Solicitante:	244000 - Dirección General de Atención a la Sociedad y Relaciones Institucionales
Oficio de Solicitud	IFAI-SE-DGASRI-0589-2010
Programa:	1. Facilitación y Vinculación
Motivo:	Presentación de los resultados de la Métrica de Transparencia 2010 que se realizará en las instalaciones del Centro de Investigaciones y Docencia Económica, ubicadas en la Carretera México – Toluca, en la segunda semana de septiembre.
Justificación:	Asiste el Comisionado Presidente del Instituto de Transparencia y Acceso a la Información Pública del Estado de Baja California y la Consejería del Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública a la Reunión Nacional de la COMAIP para conocer los resultados de la Métrica de la Transparencia 2010. Así como la revisión y conocimiento de los resultados por parte de los organismos miembros de la COMAIP. $ 16,050.00 IVA Incluido (de los cuales $ 12,300.00 son para traslado y $ 3,750.00 son para viáticos)
Total:	$ 16,050.00 IVA Incluido Se incluye un 10% Adicional para considerar eventuales ajustes en los precios. $ 17,655.00 IVA Incluido
Total con letra:	(Diecisiete mil seiscientos cincuenta y cinco pesos 00/100 M.N.) IVA Incluido

Instituto Federal de Acceso
a la Información y
Protección de Datos

PRESIDENCIA

"2010, Año de la Patria. Bicentenario del Inicio de la Independencia y Centenario del Inicio de la Revolución".

OFICIO: IFAI/JPM/0108/2010

México, D.F. a 03 de septiembre de 2010

Se hace constar que la autorización de la Comisionada Presidenta, no exime al área solicitante de cumplir con todos los trámites y requisitos que establecen, la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y la Ley Federal de Presupuesto y Responsabilidad Hacendaria.

Sin más por el momento, le envío un cordial saludo.

ATENTAMENTE

Solicita Ejecutar Partidas y Certifica Suficiencia Presupuestal Director General de Administración	Autorizó Comisionada Presidenta
Lic. Eduardo Fernández S.	Dra. Jacqueline Peschard Mariscal

INSTITUTO FEDERAL DE ACCESO A LA INFORMACION PUBLICA

Póliza No -> **1383 De Cp** **Fecha ->** **29/Oct/10**

Concepto -> **F-963 ACROM IMPRESORES SA DE CV IMPRESION 500 CARTELES 1500 PROG ALUSIVOS VIII ENC IBEROAMER PROT DTOS 12/OCT/10 P61-10**

No. Cuenta	Nombre Concepto o Movimiento	DEBE	HABER
4201-3-6-02-30-320	DIR GRAL CLASIF INFOR Y DATOS PERSONALES F-963 ACROM IMPRESORES SA DE CV 12/OCT/2010 P61-10	13,189.20	
2102-1-1-01-01-053	ACROM IMPRESORES SA DE CV F-963 IMPRES 500 CARTELES Y 1500 PROGR ALUSIVOS VIII ENC IBE ROAMERICANO PROT DTOS 12/OCT/10 P61-10		13,189.20
5204-3-6-02-30-320	DIR GRAL CLASIF INFOR Y DATOS PERSONALES F-963 ACROM IMPRESORES SA DE CV 12/OCT/2010 P61-10	13,189.20	
5203-3-6-02-30-320	DIR GRAL CLASIF INFOR Y DATOS PERSONALES F-963 ACROM IMPRESORES SA DE CV 12/OCT/2010 P61-10		13,189.20
SUMAS IGUALES ->		**26,378.40**	**26,378.40**

Hecho por :	Revisado por :	Autorizado por :	Diario No. Cp	Póliza No : 1383

SECRETARIA EJECUTIVA
DIRECCION GENERAL DE ADMINISTRACION
DIRECCIÓN DE RECURSOS FINANCIEROS
CUENTA POR PAGAR

Vale. 11 NOV.

0847000183265 69

Transf

NÚMERO DE CUENTA POR PAGAR	01383		
	DÍA	MES	AÑO
FECHA DE EXPEDICIÓN	29	10	2010
HOJA	No.	DE	
	1	1	

CUENTA PAGADORA	$	13,189.20
609889769		

(IMPORTE)

BENEFICIARIO	Acrom Impresores, S.A. de C.V.

INSTITUCIÓN BANCARIA

JUSTIFICACIÓN	Pago F-963 Impresión 500 carteles y 1,500 programas de mano alusivos al VIII Encuentro Iberoamericano Protección Datos. 12/10/2010. P61-10.

TIPO DE CUENTA
CN Cuenta Normal

Clave presupuestal	Partida	Unidad Adm.	Tipo Doc.	Factura Número	Contrato	Póliza Cheque	Concepto	Bruto	Neto
2010 06 HHE 1 4 08 00 010 E006 3N	3602	3200 DGCIDP	Factura	963	P61-10		Impresión 500 carteles y 1,500 programas de mano alusivos al VIII Encuentro Iberoamericano Protección Datos. 12/10/2010.	$13,189.20	$13,189.20

Afectación Presupuestal	(Trece Mil Ciento Ochenta y Nueve Pesos 20/100 M.N.)	Total	$ 13,189.20	$ 13,189.20
	(IMPORTE CON LETRA)	Retención	$ -	

Elaboró

María de Lourdes Carlos Manuel
Subdirector de Tesorería y Contabilidad

Revisó

Margarita Montero Rojas
Director de Recursos Financieros

Autorizó

Eduardo Fernández S.
Director General de Administración

SPEI - BANORTE - CLAVE DE RASTREO
8846 APA-720[illegible]1110037091799
11/11/2010

85. Banamex 002180023475062413

INSTITUTO FEDERAL DE ACC A LA INFOR. Y PROTECCION DE DATOS

Póliza No -> **1378 De Cp** **Fecha ->** **29/Oct/10**

Concepto -> **F-508 HECTÀREA PRODUCCIONES SA DE CV PAGO SALDO SERV INT LOG ÌSTICA VII ENC IBEROAMÈRIC PROTEC.DTOS 20/OCT/2010 C055/10**

No. Cuenta	Nombre Concepto o Movimiento	DEBE	HABER
4201-3-8-04-30-320	DIR GRAL CLASIF INFOR Y DATOS PERSONALES F-508 HECTÀREA PRODUCCIONES SA DE CV 20/OCT/2010 C055/10	1,272,705.60	
2102-1-1-01-08-016	HECTAREA PRODUCCIONES SA DE CV F-508 PGO SDO SERV INT LOGÌSTICA VII ENC IBEROAMÈRIC PROTEC .DTOS 20/OCT/2010 C055/10		1,272,705.60
5204-3-8-04-30-320	DIR GRAL CLASIF INFOR Y DATOS PERSONALES F-508 HECTÀREA PRODUCCIONES SA DE CV 20/OCT/2010 C055/10	1,272,705.60	
5203-3-8-04-30-320	DIR GRAL CLASIF DATOS PERSONALES F-508 HECTÀREA PRODUCCIONES SA DE CV 20/OCT/2010 C055/10		1,272,705.60
SUMAS IGUALES ->		**2,545,411.20**	**2,545,411.20**

Hecho por :	Revisado por :	Autorizado por :	Diario No. Cp	Póliza No : 1378

INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN
Y PROTECCIÓN DE DATOS
DIRECCIÓN GENERAL DE ADMINISTRACIÓN
DIRECCIÓN DE RECURSOS FINANCIEROS

"2010, Año de la Patria. Bicentenario del Inicio de la Independencia y Centenario del Inicio de la Revolución".

IFAI-SE-DGA-DRF-123

México, D.F. a 24 de septiembre de 2010

Lic. Eduardo Rodríguez Arias
Director de Recursos Materiales y
Servicios Generales
P R E S E N T E

Me refiero su oficio No. IFAI/SE/DGA-drmsg/666/2010, de fecha 24 de Septiembre del presente año, en el que menciona solicita se amplié el importe del compromiso presupuestal de la erogación que a continuación se menciona:

PROVEEDOR	CONCEPTO	MONTO TOTAL	PARTIDA	No. CONTRATO	PERIODO
Hectárea Producciones, S.A. de C.V.	Servicio Integral de logística en el marco del evento "VIII Encuentro Iberoamericano de Protección de Datos""	$ 1,527,870.80 IVA INCLUIDO	3804	dgcdp/096bis	Septiembre

Sobre el particular, me permito comunicar que esta dirección, ha efectuado la ampliación al compromiso por un importe de $ 252,044.80 quedando el total de $ 1,527,870.80 en la Partida que se indican, toda vez que el área solicitante menciona que esta operación corresponde al convenio modificatorio del contrato respectivo.

Sin más por el momento, reciba un cordial saludo.

ATENTAMENTE

INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS
SECRETARÍA EJECUTIVA
24 SEP 2010
10:00 hrs
DIRECCIÓN GENERAL DE ADMINISTRACIÓN
DIRECCIÓN DE RECURSOS MATERIALES Y SERVICIOS GENERALES

C.P. MARGARITA MONTERO ROJAS
DIRECTOR DE RECURSOS FINANCIEROS

C.c.p.- Eduardo Fernández S - Director General de Administración.

24.10.10 12:59

INSTITUTO FEDERAL DE ACCESO A LA INFORMACION PUBLICA

Póliza No -> **1173 De Cp** **Fecha ->** **29/Sep/10**

Concepto -> **HECTÀREA PRODUCCIONES SA DE CV PGO ANT 20%MONTO TOTAL DE CON F ART 48 LAASSP Y ART.81 PV RLAASSP L.ORNELASC055/10**

No. Cuenta	Nombre Concepto o Movimiento	DEBE	HABER
4201-3-8-04-30-320	DIR GRAL CLASIF INFOR Y DATOS PERSONALES HECTÀREA PRODUCCIONES SA DE CV PGO ANT 20%MONTO TOTAL DE CON F ART 48 LAASSP Y ART.81 PV RLAASSP L.ORNELAS C055/10	255,165.20	
2102-1-1-01-08-016	HECTAREA PRODUCCIONES SA DE CV PGO ANT 20%MONTO TOTAL DE CONF ART 48 LAASSP Y ART.81 PV RLA ASSP L.ORNELAS C055/10		255,165.20
5204-3-8-04-30-320	DIR GRAL CLASIF INFOR Y DATOS PERSONALES HECTÀREA PRODUCCIONES SA DE CV PGO ANT 20%MONTO TOTAL DE CON F ART 48 LAASSP Y ART.81 PV RLAASSP L.ORNELAS C055/10	255,165.20	
5203-3-8-04-30-320	DIR GRAL CLASIF DATOS PERSONALES HECTÀREA PRODUCCIONES SA DE CV PGO ANT 20%MONTO TOTAL DE CON F ART 48 LAASSP Y ART.81 PV RLAASSP L.ORNELAS C055/10		255,165.20
SUMAS IGUALES ->		**510,330.40**	**510,330.40**

Hecho por :	Revisado por :	Autorizado por :	Diario No.	Póliza No :
			Cp	1173

SECRETARIA EJECUTIVA
DIRECCION GENERAL DE ADMINISTRACION
DIRECCIÓN DE RECURSOS FINANCIEROS
CUENTA POR PAGAR

NUM. DE CUENTA POR PAGAR	01173		
	DIA	MES	AÑO
FECHA DE EXP.	29	9	2010
HOJA	No.	DE	
	1	1	

CUENTA PAGADORA	$ 255,165.20
609889769	(IMPORTE)

BENEFICIARIO	Hectárea Producciones, S.A. de C.V.

INSTITUCION BANCARIA

JUSTIFICACION	Pago Anticipo 20% del monto total C055/10 de conformidad con Art. 48 LAASSP y Art. 81 P.V RLAASSP. (L. Ornelas)

TIPO DE CUENTA
CN Cuenta Normal

Clave presupuestal	Partida	Unidad Adm.	Tipo Doc.	Factura Número	Contrato	Póliza Cheque	Concepto	Bruto	Neto
2010 06 HHE 1 4 08 00 010 E006 1	3804	3200 DGCIDP	Otros		C055/10		Pago Anticipo 20% del monto total C055/10 de conformidad con Art. 48 LAASSP y Art. 81 P.V RLAASSP. (L. Ornelas)	$255,165.20	$255,165.20

Afectación Presupuestal	(Doscientos Cincuenta y Cinco Mil Ciento Sesenta y Cinco Pesos 20/100 M.N.)	Total	$ 255,165.20	$ 255,165.20
	(IMPORTE CON LETRA)	Retención	$ -	

Elaboró

María de Lourdes Carlos Manuel
Subdirector de Tesorería y Contabilidad

Revisó

Margarita Montero Rojas
Director de Recursos Financieros

Autorizó

Eduardo Fernández S.
Director General de Administración

5149

IFAI

INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS

TITULO: CONTRATACION DE SERVICIO PARA EL DISEÑO DE LOGOTIPO Y CARTEL ALUSIVO AL VII ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS

FECHA: 9 DE SEPTIEMBRE DE 2010.

MARÍA DEL CARMEN RIVERO VALLE Y/O DEGITOS	SAHANTHA BELAUKAZÁN GARCÍA Y/O ENTERTAINMENT	MARIAN RIQUELME Y/O ZITRUS

PARTIDA	CONCEPTO	CANTIDAD	UNIDAD	PRECIO UNITARIO	PRECIO TOTAL	PRECIO UNITARIO	PRECIO TOTAL	PRECIO UNITARIO	PRECIO TOTAL
1	Diseño de logotipo	1	servicio	$15,000.00	$15,000.00	$22,000.00	$22,000.00	$16,500.00	$16,500.00
2	Diseño del cartel promocional	1	servicio	$8,000.00	$8,000.00	$9,300.00	$9,300.00	$12,200.00	$12,200.00
	SUBTOTAL				**$23,000.00**		**$31,300.00**		**$28,700.00**
	I.V.A.				**$3,680.00**		**$5,008.00**		**$4,592.00**
	TOTAL				**$26,680.00**		**$36,308.00**		**$33,292.00**

INSTITUTO FEDERAL DE ACCESO A LA INFORMACION PUBLICA

Póliza No -> **1253 De Cp** **Fecha ->** **8/Oct/10**

Concepto -> **F-322 MARIA DEL CARMEN RIVERO VALLS SERV DISEÑO CARTEL PARA VIII ENCUENTRO IBEROAMER PROT DTOS 22/SEPT/2010 P59/10**

No. Cuenta	Nombre Concepto o Movimiento	DEBE	HABER
4201-3-4-13-50-500	IFAI F-322 MARIA DEL CARMEN RIVERO VALLS 22/SEPT/2010 P59/10	26,680.00	
2102-1-1-01-19-064	RIVERO VALLS MARIA DEL CARMEN F-322 SERV DISEÑO CARTEL PARA VIII ENC IBEROAMER PROT DTOS 2 2/SEPT/2010 P59/10	2,453.33	
2102-1-1-01-19-064	RIVERO VALLS MARIA DEL CARMEN F-322 SERV DISEÑO CARTEL PARA VIII ENC IBEROAMER PROT DTOS 2 2/SEPT/2010 P59/10		26,680.00
2101-1-1-02-00-000	IVA RETENIDO A TERCEROS F-322 MARIA DEL CARMEN RIVERO VALLS 22/SEPT/2010 P59/10		2,453.33
5204-3-4-13-50-500	IFAI F-322 MARIA DEL CARMEN RIVERO VALLS 22/SEPT/2010 P59/10	26,680.00	
5203-3-4-13-50-500	IFAI F-322 MARIA DEL CARMEN RIVERO VALLS 22/SEPT/2010 P59/10		26,680.00

SUMAS IGUALES -> **55,813.33** **55,813.33**

Hecho por :	Revisado por :	Autorizado por :	Diario No. Cp	Póliza No : 1253

SECRETARIA EJECUTIVA
DIRECCION GENERAL DE ADMINISTRACION
DIRECCIÓN DE RECURSOS FINANCIEROS
CUENTA POR PAGAR

Transf Mifel
Jueves 28 oct.

NÚMERO CUENTA POR PAGAR	01253

FECHA	DÍA	MES	AÑO
	8	10	2010
HOJA	No.	DE	
	1	1	

0547000179849 83

CUENTA PAGADORA	$ 24,226.67
609889769	

(IMPORTE)

BENEFICIARIO	María del Carmen Rivero Valls

INSTITUCIÓN BANCARIA

JUSTIFICACIÓN	Pago F-322 Servicio de diseño de logotipo y diseño de cartel para VIII Encuentro Iberoamericano de Protección de Datos. 22/09/2010. P59-10.

TIPO DE CUENTA
CN Cuenta Normal

Clave presupuestal	Partida	Unidad Adm.	Tipo Doc.	Factura Número	Contrato	Póliza Cheque	Concepto	Bruto	Neto
2010 06 HHE 1 4 08 00 010 E006 1N	3413	5000 IFAI	Factura	322	P59-10		Servicio de diseño de logotipo y diseño de cartel para VIII Encuentro Iberoamericano de Protección de Datos. 22/09/2010.	$26,680.00	$24,226.67

Afectación Presupuestal	(VeintiCuatro Mil Doscientos Veinti Seis Pesos 67/100 M.N.)	TOTAL	$ 26,680.00	$ 24,226.67
	(IMPORTE CON LETRA)	RETENCIÓN	$ 2,453.33	

Elaboró

María de Lourdes Carlos Manuel
Subdirector de Tesorería y Contabilidad

Revisó

Margarita Montero Rojas
Director de Recursos Financieros

Autorizó

Eduardo Fernández S.
Director General de Administración

SPEI- BBVA BANCOMER - CLAVE DE RASTREO
BB46APAC 201010280036425875
28/10/2010

66. Banca Mifel SA. 042180000001174554

Instituto Federal de Acceso a la Información y Protección de Datos

PRESIDENCIA

"2010, Año de la Patria. Bicentenario del Inicio de la Independencia y Centenario del Inicio de la Revolución".

OFICIO: IFAI/JPM/0123bis/2010

México, D.F. a 23 de septiembre de 2010

Lic. Eduardo Fernández Sánchez
Director General de Administración
P R E S E N T E

Con la finalidad de dar cumplimiento a lo dispuesto en el Capítulo IV, Artículo 63 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, que a la letra dice: "Los titulares de los ejecutores de gasto autorizarán las erogaciones por concepto de gastos de orden social, congresos, convenciones,...", le informo que se autoriza ejercer las siguientes partidas como a continuación se indica:

Partida 7502 "Gastos por Servicios de Traslado de Personas"

Unidad Solicitante:	320000 - Dirección General de Clasificación y Datos Personales.
Oficio de Solicitud:	IFAI-SA-DGCDP-105-10
Programa:	6. Desarrollo Institucional
Motivo:	Cubrir el monto generado por el servicio de hospedaje y alimentación para expositores en el hotel sede del evento VIII Encuentro Iberoamericano de Protección de Datos que tendrá lugar el próximo miércoles 29 y jueves 30 de septiembre.
Justificación:	Hospedaje y alimentación de los ponentes y miembros de la Red Iberoamericana de Protección de Datos Personales que participaran en el VIII Encuentro Iberoamericano.
Total:	$ 620,000.00 IVA incluido
Total con letra:	(Seiscientos veinte mil pesos 00/100 M.N.) IVA incluido

Unidad Solicitante:	201000 - Dirección de Asuntos Internacionales
Oficio de Solicitud	IFAI/SE/DAI/T/0902/2010
Programa:	6. Desarrollo Institucional
Motivo:	Traslado de ponentes e invitados internacionales que participarán en el VIII Encuentro Iberoamericano de Protección de Datos.
Justificación:	Traslado de ponentes e invitados internacionales entre los días 27 de septiembre y 2 de octubre, que participaran en el VIII Encuentro Iberoamericano de Protección de Datos, que tiene como propósito el intercambio de experiencias en materia de privacidad y protección de datos entre los países de Iberoamérica. El encuentro se realizara en el Hotel Royal pedregal ubicado en Periférico Sur No. 463, Col. Jardines de la Montaña, Delegación Tlalpan, C.P. 14210, México, D.F.
Total:	$ 237,025.79 IVA incluido
Total con letra:	(Doscientos treinta y siete mil veinticinco pesos 79/100 M.N.) IVA incluido

Se hace constar que la autorización de la Comisionada Presidenta, no exime al área solicitante de cumplir con todos los trámites y requisitos que establecen, la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y la Ley Federal de Presupuesto y Responsabilidad Hacendaria.

Sin más por el momento, le envío un cordial saludo.

A T E N T A M E N T E

Solicita, Revisa, Autoriza y Captura Suficiencia Presupuestal Director General de Administración	Autorizo Comisionada Presidenta
Lic. Eduardo Fernández S.	Dra. Jacqueline Peschard Mariscal

INSTITUTO FEDERAL DE ACCESO A LA INFORMACION PUBLICA

Póliza No -> **1215 De Cp** **Fecha ->** **1/Oct/10**

Concepto -> **F-277001 RESTAURANTES RICLER SA DE CV SERV INT P/DES ACTO PR OTOCOL VIII ENC IBEROAMÈR DE PROTEC DTOS 29/SEPT/2010 P64/10**

No. Cuenta	Nombre Concepto o Movimiento	DEBE	HABER
4201-3-8-04-50-500	IFAI F-277001 RESTAURANTES RICLER SA DE CV S 29/SEPT/2010 P64/10	45,793.87	
2102-1-1-01-19-066	RESTAURANTES RICLER, SA DE CV F-277001 SERV INT P/DES ACTO PROTOCOL VIII ENC IBEROAMÈR DE PROTEC DTOS 29/SEPT/2010 P64/10		45,793.87
5204-3-8-04-50-500	IFAI F-277001 RESTAURANTES RICLER SA DE CV 29/SEPT/2010 P64/10	45,793.87	
5203-3-8-04-50-500	IFAI F-277001 RESTAURANTES RICLER SA DE CV 29/SEPT/2010 P64/10		45,793.87
SUMAS IGUALES ->		**91,587.74**	**91,587.74**

Hecho por :	Revisado por :	Autorizado por :	Diario No.	Póliza No :
			Cp	1215

SECRETARÍA EJECUTIVA
DIRECCION GENERAL DE ADMINISTRACION
DIRECCIÓN DE RECURSOS FINANCIEROS
CUENTA POR PAGAR

NUM. DE CUENTA POR PAGAR	01215		
	DÍA	MES	AÑO
FECHA DE EXP.	1	10	2010
HOJA	No.	DE	
	1	1	

CUENTA PAGADORA	$ 45,793.87
609889769	(IMPORTE)

BENEFICIARIO	Restaurantes Ricler, S.A. De C.V.

INSTITUCIÓN BANCARIA

JUSTIFICACIÓN	Pago F-277001 Servicio integral para desarrollo del acto protocolario del "VIII Encuentro Iberoamericano de Protección de Datos". 29/09/2010. P64-10.

TIPO DE CUENTA
CN Cuenta Normal

Clave presupuestal	Partida	Unidad Adm.	Tipo Doc.	Factura Número	Contrato	Póliza Cheque	Concepto	Bruto	Neto
2010 06 HHE 1 4 08 00 010 E006 1N	3804	5000 IFAI	Factura	277001	P64-10		Servicio integral para desarrollo del acto protocolario del "VIII Encuentro Iberoamericano de Protección de Datos". 29/09/2010.	$45,793.87	$45,793.87

Afectación Presupuestal	(Cuarenta y Cinco Mil Setecientos Noventa y Tres Pesos 87/100 M.N.)	Total	$ 45,793.87	$ 45,793.87
	(IMPORTE CON LETRA)	Retención	$ -	

Elaboró

María de Lourdes Carlos Manuel
Subdirector de Tesorería y Contabilidad

Revisó

Margarita Montero Rojas
Director de Recursos Financieros

Autorizó

Eduardo Fernández S.
Director General de Administración

82 Banamex

002180065073576932

SPEI BBVA BANCOMER CLAVE DE RASTREO
BBVAPAC 20101001001003521840
01/10/2010

[redacted]JTO FEDERAL DE ACCESO A LA INFORMACION PUBLICA

Póliza No -> **1444 De Cp** **Fecha ->** **11/Nov/10**

Concepto -> **F-46908 ALGASE SA DE CV SERV HOSP Y ALIM P/REALIZ DELVIII EI PD LOS DÌAS 27-30/OCT/2010 P63-10 OF AUT.JPM/0123BIS/2010**

No. Cuenta	Nombre Concepto o Movimiento	DEBE	HABER
4201-7-5-02-30-320	DIR GRAL CLASIF INFOR Y DATOS PERSONALES F-46908 ALGASE SA DE CV 27-30/OCT/2010. P63-10 OF AUT.JPM/0 123BIS/2010	522,573.80	
2102-1-1-01-01-061	ALGASE SA DE CV F-46908 SERV HOSP Y ALIM P/REALIZ DELVIII EIPD LOS DÌAS 27-3 0/OCT/2010 P63-10 OF AUT.JPM/0123BIS/2010		522,573.80
5204-7-5-02-30-320	DIR GRAL CLASIF INFOR Y DATOS PERSONALES F-46908 ALGASE SA DE CV 27-30/OCT/2010 P63-10 OF AUT.JPM/012 3BIS/2010	522,573.80	
5203-7-5-02-30-320	DIR GRAL CLASIF INFOR Y DATOS PERSONALES F-46908 ALGASE SA DE CV 27-30/OCT/2010 P63-10 OF AUT.JPM/012 3BIS/2010		522,573.80

SUMAS IGUALES -> **1,045,147.60** **1,045,147.60**

Hecho por :	Revisado por :	Autorizado por :	Diario No. Cp	Póliza No : 1444

SECRETARÍA EJECUTIVA
DIRECCION GENERAL DE ADMINISTRACION
DIRECCIÓN DE RECURSOS FINANCIEROS
CUENTA POR PAGAR

0547000184954 8

Vac. 25 Nov.

NÚM. DE CUENTA POR PAGAR	01444		
	DÍA	MES	AÑO
FECHA DE EXP.	11	11	2010
HOJA	No.	DE	
	1	1	

CUENTA PAGADORA	$ 522,573.80
609889769	

(IMPORTE)

BENEFICIARIO	Algase, S.A. de C.V.

INSTITUCIÓN BANCARIA

JUSTIFICACIÓN	Pago F-469083 Servicio hospedaje y alimentación para realización del VIII EIPD durante los días 27-30 octubre 2010. P63-10. Of. aut. JPM/0123bis/2010.

TIPO DE CUENTA
CN Cuenta Normal

Clave presupuestal	Partida	Unidad Adm.	Tipo Doc.	Factura Número	Contrato	Póliza Cheque	Concepto	Bruto	Neto
2010 06 HHE 1 4 08 00 010 E006 6	7502	3200 DGCIDP	Factura	469083	P63-10		Servicio hospedaje y alimentación para realización del VIII EIPD durante los días 27-30 octubre 2010. Of. aut. JPM/0123bis/2010.	$522,573.80	$522,573.80

Afectación Presupuestal	(Quinientos VeintiDos Mil Quinientos Setenta y Tres Pesos 80/100 M.N.)	Total	$ 522,573.80	$ 522,573.80
	(IMPORTE CON LETRA)	Retención	$ -	

Elaboró

María de Lourdes Carlos Manuel
Subdirector de Tesorería y Contabilidad

Revisó

Margarita Montero Rojas
Director de Recursos Financieros

Autorizó

Eduardo Fernández S.
Director General de Administración

5431