

México, D.F. a 05 de Noviembre de 2004

INFORME SOBRE LA PARTICIPACIÓN DEL IFAI EN EL “SEGUNDO SEMINARIO INTERNACIONAL DE PROTECCIÓN DE DATOS PERSONALES” Y EN EL “ENCUENTRO INTERNACIONAL DE DATOS PERSONALES EN LAS TELECOMUNICACIONES”

**BUENOS AIRES, ARGENTINA
26-29 DE OCTUBRE DE 2004**

INTRODUCCIÓN

- I. LA PROTECCIÓN DE LOS DATOS PERSONALES EN EL SISTEMA BANCARIO Y FINANCIERO
- II. LA PROTECCIÓN DE LOS DATOS PERSONALES, INTEGRACIÓN REGIONAL O INTERNACIONAL
- III. LA PROTECCIÓN DE DATOS Y LA INFORMACIÓN CREDITICIA
- IV. LA PROTECCIÓN DE LOS DATOS PERSONALES EN EL ÁMBITO DE LA SALUD: LOS DATOS SENSIBLES
- V. EL REGISTRO NACIONAL DE BANCO DE DATOS PÚBLICOS Y PRIVADOS
- VI. ASPECTOS TÉCNICOS DE LAS COMUNICACIONES ELECTRÓNICAS PARA NO TÉCNICOS.
- VII. RETENCIÓN Y PRESERVACIÓN DE DATOS DE TRÁFICO. DATOS DE LOCALIZACIÓN
- VIII. SITIOS DE INTERÉS

INTRODUCCIÓN

Con la promulgación de la ley 25.326, Argentina se convirtió hace dos años en el primer país de Latinoamérica en establecer una legislación específica sobre la protección de los datos personales. El régimen de privacidad adoptado por la nación sudamericana cumple en buena medida con los principios establecidos por la Unión Europea, por lo que, en lo que hace a América Latina, tal país se puso a la cabeza en materia de protección de datos personales cuando implementó el habeas data.

La Dirección Nacional de Protección de Datos Personales es el organismo gubernamental responsable del cumplimiento de la Ley mencionada, misma que está en el ámbito del Ministerio de Justicia de la República Argentina. Cabe destacar que el país aludido ha sido declarado sede de la 26^o Conferencia Internacional de Protección de Datos Personales a celebrarse en el 2005.

Como parte fundamental en la implementación de la regulación del derecho fundamental a la tutela de los datos de carácter personal, Argentina, como el país latinoamericano con mayor avance en la protección de tales datos realizó congresos para intercambiar experiencias en la materia. En ese contexto, Lina Ornelas Nuñez, Directora General de Clasificación y Datos Personales del Instituto Federal de Acceso a la Información Pública y Cuauhtémoc Hinojosa Herrera, Director de Clasificación y Datos Personales “B” del mismo Instituto, acudieron al Segundo Seminario Internacional sobre Protección de Datos Personales y al Encuentro Internacional: Protección de Datos Personales en Telecomunicaciones, celebrados en Buenos Aires, los días 26, 27, 28 y 29 de octubre de 2004.

En las conferencias se tocaron temas relacionados con aspectos técnicos en las comunicaciones electrónicas, rubros relativos a la retención y preservación de datos de tráfico, así como desafíos y peligros de las nuevas tecnologías. Por otra parte, se trató el tópico de la protección de los datos personales en el sistema bancario y financiero, en las transferencias internacionales, en el ámbito de la salud y el tratamiento de tales datos en los registros públicos y privados. Una de las charlas que más interesó a los representantes del IFAI, fue la discusión sobre el uso de la información personal de las instituciones financieras y bancarias con motivo del debate que actualmente se realiza en México sobre abrir la información concerniente a los secretos.

La asistencia del IFAI a la conferencia fue de crucial importancia en virtud de que el extenso abanico de los temas a debatir, permitió el intercambio de ideas y vivencias entre las autoridades de protección de datos, representantes de organizaciones internacionales provenientes de los sectores públicos, privados y académicos. Con la participación del Instituto no sólo se trata de impulsar y apoyar la protección de datos personales en México, si no también de que haya un ambiente de conocimiento en la sociedad y en las empresas sobre la importancia de la privacidad, por lo cual se acordó la celebración de convenios de colaboración entre el IFAI, la Agencia Española de Protección de Datos Personales y la Dirección Nacional de Protección de Datos Personales de Argentina.

SEGUNDO SEMINARIO INTERNACIONAL DE PROTECCIÓN DE DATOS PERSONALES

**Buenos Aires, Argentina
26 y 27 de octubre de 2004**

I. LA PROTECCIÓN DE LOS DATOS PERSONALES EN EL SISTEMA BANCARIO Y FINANCIERO

Moderador: JUAN ANTONIO TRAVIESO

La Dirección Nacional de Protección de Datos Personales lleva meses de diálogo con *spammers*, empresas de *telecom* y reguladores gubernamentales. Destaca que la condición de pobreza no debe divulgarse, por ello, hace énfasis en la protección de los datos personales de los pobres.

El Derecho regional se ha resistido a la protección de datos personales, por lo que los objetivos de la Dirección se han forjado en razón de acelerar el aprendizaje en la materia. La propuesta del Director radica en que se debe conciliar el *opt-in* con el *opt-out*. Cabe destacar como una de las prioridades de la Dirección, la acogida de la estipulación para que Argentina sea la sede de la Conferencia Internacional de Datos Personales en el 2006.

JORGE NUNES. GERENTE DEPARTAMENTAL DE ORGANIZACIÓN Y PROCESOS DEL BANCO DE LA NACIÓN DE ARGENTINA

El ponente resaltó la existencia de vulnerabilidades sobre fraudes, hardware y política de seguridad informática. De acuerdo a las atribuciones de la Dirección General del Banco de Nación de Argentina, se organiza la seguridad con la confidencialidad de la información se respeta y sólo se otorga acceso con autorización; por otra parte, se prevén los requisitos de integridad y disponibilidad de los datos personales.

Los actores en estos procesos de negocio son los propietarios de datos y los usuarios que acuden a los datos por facultad delegada áreas de tecnologías.

| Controles | Confiere a | Protección |
|------------------|-------------------|-------------------|
| Interna | Directores | Estricto |
| Interna | Empleados | Suficiente |
| Pública | Comunidad | Mínimo |

Para garantizar la seguridad en los datos personales, es necesario contestar a las preguntas qué, quién y cómo se puede acceder. Los aspectos de seguridad física, lógica, administrativa deben prevalecer a la “necesidad de conocer”. La Unidad de Información

Financiera (UIF) del Banco Central de Argentina se caracteriza por sus medidas en materia de seguridad de los datos personales.

El riesgo debe acotarse a la falla para potenciales pérdidas, por lo que se debe organizar la legislación. El control tecnológico, las políticas de seguridad informática y el sistema de aplicación de negocios evitan los riesgos y paradigmas. Por otra parte, los aspectos básicos en seguridad informática son confidencialidad, integridad y disponibilidad. En conclusión, la protección de datos debe de formar parte del proceso y seguridad de las empresas.

EVELINA SARRAILH, DIRECTORA DE SERVICIOS JURÍDICOS DEL BBVA BANCO FRANCÉS S.A.

Sarrailh abundó en la forma en que las disposiciones emitidas por el BBVA en materia de protección de datos personales, se adecuan al marco jurídico de las entidades financieras en Argentina. Tales regulaciones son la Ley de entidades financieras 21520; la Ley de lavado de dinero permite acceder a información sobre créditos; la Ley de protección de datos y por último, la Circular Banco Central de la República Argentina respecto a la clasificación de clientes

Todo lo anterior bajo el secreto bancario protege la confidencialidad. La información que reciben las autoridades financieras y el tratamiento de datos personales permiten que unidos configuren perfiles. Las declaraciones patrimonial y fiscal tienen consecuencias en el tratamiento de la información que reciben las entidades financieras.

La información de obligaciones activas son transferidas al Banco Central y los bancos le informan sobre los datos de sus clientes. Los informes que reciben las entidades financieras los solicitan al Banco Central. Tales documentos contienen el nombre, fecha de nacimiento, número de DEC, CUIT/WIL, domicilio, estado civil, nombre de los padres, datos del cónyuge, profesión/actividad, entre otros. Estos informes que recogen las bases de datos de sociedades de liquidación, las cuales implican los requerimiento de los clientes para su tratamiento.

Para Evelina Sarrailh, fue importante señalar que Argentina cumple con las condiciones de protección de datos personales conforme al Protocolo 95 de la Comisión Europea.

CARLOS M. VILLEGAS, ABOGADO. LICENCIADO EN ECONOMÍA. MASTER EN FINANZAS (CEMA). SOCIO DEL ESTUDIO NICHOLSON & CANO ABOGADOS

En Argentina existe el habeas data financiero, el cual se regula de la siguiente manera: El artículo 43 de la Constitución protege a la privacidad de los individuos. Por otra parte, el secreto bancario establecido en el artículo 39 de la Ley 21.526 de Entidades Financieras, asimismo, el artículo 26 de la Ley 25.326 de Protección de Datos Personales trata a la información crediticia

Al respecto, el ponente destacó la importancia de las comunicaciones “A” 2729 y la “B” 2950 del Banco Central de Argentina. En particular, el punto 8.1 de la primera. Esa regulación establece la facultad para el cliente cuando éste solicite un crédito tenga previo conocimiento que su conducta será calificada. Asimismo, debe saber sobre sus derechos a conocer y rectificar sus datos personales.

Los actores de esta situación son en primer lugar los deudores del sistema financiero, la actividad financiera y el banco central. En este sentido, las entidades crediticias deben informar sobre cuatro aspectos, fundamentalmente la última clasificación, los fundamentos para calificar, el importe total de deudas, así como las últimas calificaciones disponibles.

Para los deudores de cartera comercial y de cartera de consumo, aseveró Villegas, existe una forma de acceso al centro de deudores del sistema financiero, el cual consiste en el ingreso con la clave de identificación fiscal, el nombre del deudor, monto de la deuda y calificación de éste.

En una situación normal, las entidades crediticias evalúan el riesgo potencial sobre el alto riesgo de insolvencia, lo cual podría ser irrecuperable por disposición técnica. La solicitud se realiza vía Internet a través de un CUIT (cédula de información). Para efectos de defensa al deudor, existe una etapa prejudicial frente a la entidad financiera cuando requiera corregir sus datos personales, posteriormente, la etapa judicial consiste en una comunicación post corrección de un medio que tenga similar poder de divulgación.

Por lo anterior, con estos procedimientos se permite al particular el acceso al registro de datos, su actualización y eventual corrección. Asimismo, el acceso a la información respecto de las obligaciones de las entidades financieras a comunicarles su calificación, obligación de informar sobre la base de datos, acerca de quienes tienen el derecho de acceder a ellas, los deudores o las entidades.

II. LA PROTECCIÓN DE LOS DATOS PERSONALES, INTEGRACIÓN REGIONAL O INTERNACIONAL

PATRICIA VACA NARVAJA, SUBSECRETARIA DE DEFENSA DE LA COMPETENCIA Y DEFENSA DEL CONSUMIDOR

Patricia Vaca trató el tema de la organización de la defensoría de los consumidores argentinos. Al respecto, la COFEDEC se integra con todas las autoridades provinciales y su función consiste en hacer una divulgación de la educación del consumidor. La Ley de Protección al Consumidor impone la obligación a los proveedores de promover la cultura de consumidores, es decir, que estos estén informados sobre el destino de sus datos.

EUGENIO CURIA, CONSEJERO LEGAL DEL MINISTERIO DE RELACIONES EXTERIORES, COMERCIO INTERNACIONAL Y CULTO

Argentina tiene un nivel adecuado de protección basado en el sistema de supervisión entre pares en la defensa de los consumidores. El país en mención obtuvo el reconocimiento de la

Unión Europea para la protección de datos personales. En este entendido, lo que la comunidad transfiere es seguro en ese país, por lo que las decisiones pueden suspenderse si algún Estado miembro demuestra baja protección.

Eugenio Curia enfatizó que la supervisión entre los países prevalece para saber si se cumplen los requisitos de protección. En este sentido, empresas como “ASSET” vigilan negocios con la Unión Europea. El efecto principal es la deslocalización de empresas por el uso de *call center*.

MÓNICA LUCERO DE NOFAL, DIRECTORA DE FISCALIZACIÓN, CONTROL Y DEFENSA DEL CONSUMIDOR DE LA PROVINCIA DE MENDOZA Y COORDINADORA DEL CONSEJO FEDERAL DE DEFENSA DEL CONSUMIDOR (COFEDEC)

La ponente señaló que con la aprobación de la Ley de Defensa del Consumidor de 1990, sólo se ingresa al registro de morosos, únicamente lo que se pactó entre el consumidor y el proveedor. En este sentido surge la interrogante: ¿cuándo los datos exclusivos se vuelven excesivos y cómo definirlos? En este sentido, se suma a la propuesta al régimen de la evitar dar a conocer un dato excesivo.

CARLOS ALBERTO VANELLA, DIRECTOR DE DEFENSA DEL CONSUMIDOR, SUBSECRETARIO DE DEFENSA DE LA COMPETENCIA Y DEFENSA DEL CONSUMIDOR

En la opinión de Carlos Vanella, el resumen de la tarjeta de crédito es el ADN del comercio, con ello se conocen los perfiles de consumo que incluyen los lugares de compra, los tipos de producto, la periodicidad y el nivel de gasto. La defensa del consumidor es la defensa del ser humano como tal, por lo que es necesario evitar el manejo desproporcionado de sus datos personales.

Un rubro interesante es el de la confrontación entre datos sanos contra datos enfermos, inclusive, aun negando el envío de datos se confirman o consolidan nuevas bases de datos. Respecto a las sociedades de información, estas contienen datos como el comportamiento empresario, la actitud frente al conflicto, respeto a normas ambientales y la obligación de proveedores para consultar bases de datos crediticios.

III. LA PROTECCIÓN DE DATOS Y LA INFORMACIÓN CREDITICIA

ALFREDO VICENS, PRESIDENTE DE LA CÁMARA DE EMPRESAS DE INFORMACIÓN COMERCIAL (CEIC)

El expositor, como parte del grupo consultivo de la Dirección Nacional de Protección de Datos Personales, afirma que, para el caso de la información crediticia, los principales

aspectos que se manejan son la morosidad financiera y comercial, la observación de incumplimiento y el compartimiento de pago. El registro de información crediticia contempla a los deudores del sistema financiero, de entidades, liquidaciones y de entidades financieras de cheques rechazados. En cuanto a información judicial, las fuentes que se manejan son de acceso público, tales como: los boletines oficiales, novedades judiciales, juicios, quiebras, concursos y mediaciones

Por otra parte, existen más fuentes públicas de información crediticia como lo son la AFIP, IGJ, registros y el SRT. Para plantear estas cuestiones, los tipos de informes que se entrega a los titulares de los datos personales son la historia de crédito */bureau*, los informes de afectaciones: comerciales, de estados patrimoniales, registral-verificación laboral y domiciliario.

Para el ponente, la información comercial no es lo más perjudicial para el individuo, aunque recalcó, es necesario tutelar el acceso conforme a las exigencias del marco regulatorio.

En cuanto al derecho al olvido, Alfredo Vicens, señaló aún no se tienen parámetros sobre la manera de computarlos. En este sentido, la regulación de uso de los datos comerciales son los postulados básicos para establecer que el dato comercial no es dato sensible, sin embargo, merece tutela el acceso. Vicens precisó que el sector privado ha registrado más avances que el sector público, por lo que los compromisos exigen adecuar importe mínimo de los centrales de riesgo.

GUSTAVO BRICCHI, GERENTE DE GESTIÓN DE LA INFORMACIÓN DEL BANCO CNETRAL DE LA REPÚBLICA ARGENTINA

Gustavo Bricchi se llama así mismo fundamentalista del acceso a la información (flujo de datos personales) y cree en la necesidad de consultar las bases para sobre entender a los clientes.

Por otra parte manifiesta que las bases de datos que administran el buró de crédito contienen el control de deudores, control de cheques rechazados, control de cheques inhabilitados y control de letras de cambio rechazadas. Asimismo, se establecen mecanismos de control de deudores del servicio financiero: subproducto de normas potenciales, reclasificación obligatoria, instrumento disciplinario de mercado.

Respecto al habeas data, sostiene que es útil, sin embargo, considera que gente que no pagó desaparece de las bases de datos mediante tal procedimiento, derivado de la falta de criterios precisos de los jueces que no han sabido distinguir entre deuda vencida y no vencida, ello permitiría no incurrir en violaciones a la protección de datos personales.

PEDRO M. PÉREZ, PRESIDENTE DE LA FEDERACIÓN DE ENTIDADES EMPRESARIAS DE INSTITUTOS DE INFORMACIONES COMERCIALES DE LA REPÚBLICA ARGENTINA

Pedro Pérez narró antecedentes de los Institutos de Informaciones Comerciales, mismos que se integraron con bases de datos crediticios. Para brindar a los empresarios asociados, información valiosa y relevante para sus funciones, estas asociaciones civiles tienen estatutos o reglamentarios, además de asambleas.

Las bases se llenan de datos de la información que les den los otros asociados con la finalidad de obtener “orientación en el otorgamiento del crédito y normalización de su uso”. Con ello, no pretende interdicción o inhabilitación civil o comercial si no sólo informes orientadores, los cuales no son obligatorios. Cabe señalar que antes de la entrada en vigor de la ley se le daba acceso a la información sólo a los titulares.

IV. LA PROTECCIÓN DE LOS DATOS PERSONALES EN EL ÁMBITO DE LA SALUD. LOS DATOS SENSIBLES

CLAUDIA CAZAUX, GERENTE DE INVESTIGACIÓN CLÍNICAS Y REPRESENTANTE DE FARMACOVIGILANCIA, LABORATORIOS ABBOT ARGENTINA S.A.

La ponente señala que los datos no pertenecen a las industrias, por lo que ficheros privados y públicos pertenecientes a hospitales, consultorías, laboratorios diagnóstico por imagen, deben estar registrados de manera disociada.

El departamento médico representado por Cazaux, según señala ella misma, trata datos personales como el genoma humano, de manera disociada. En el caso de farmacovigilancia en donde se hacen perfiles de bioseguridad la información se trata con la mayor seguridad posible.

En el tratamiento de estos datos sensibles existen programas de soporte al paciente. En este sentido, en el tratamiento de tales datos por las empresas participan los proveedores, productos, servicios, recursos humanos y clientes.

Para la ponente, el establecimiento del límite de la sensibilidad del dato radica en el consentimiento informado y destrucción de los datos. Por otra parte, las transferencias de datos deben respetar los diferentes niveles de protección, asimismo, la recaudación del consentimiento informado debe ser con plazos y la destrucción de datos debe vigilar a los aspectos involucrados, para ello, existen niveles sectoriales como los códigos institucionales, políticas comparativas y procedimientos operativos estándar.

Los desafíos están en la difusión y capacitación del personal para consolidar posiciones responsables.

MARÍA FERNÁNDEZ FREIRE, GERENTE THYWILL LATAM SOLUTION S.R.L.

María Fernández, al abordar el tema de los expedientes clínicos, señaló que los mismos deben estar contenidos en una sola base de datos, para lo cual se debe establecer una regulación específica.

La ponencia consistió en la posibilidad de trazar el *back-up*. Sin embargo, subsiste la problemática del multipersonal que da seguimiento al paciente. Los expedientes clínicos sólo deben estar contenidos en una sola base de datos de regulada.

Al tocar el tema de la disociación de datos personales en el área de los estudios fármacobiólogos, la ponente señaló los casos de la farmacogenómica –identificación de los genes involucrados en determinar la respuesta a un medicamento determinado— y la farmacogenética –estudio de cómo la persona responde en forma diferente a medicamentos debido a su herencia— persiste la interrogante si la disociación debe ser absoluta o si es posible permitir la reidentificación.

El método de disociación en el área médica es muy delicado. El control alto de seguridad en la disociación hace que se sientan “libres”. La interrogante radica en qué pasa con los efectos adversos para volver a identificar. Por ello, debe existir un nivel razonable de disociación. La industria debe admitir que no pueden ser absolutamente disociados, ello también sucede en la transferencia de datos internacionales. El importador debe admitir exigencias del país de origen por los convenios.

Respecto al habeas data, señaló que la industria farmacéutica requiere del consentimiento de los pacientes para recabar información. En la recolección del consentimiento se debe establecer la finalidad concreta, por lo que no es suficiente establecer “ensayos clínicos”. Asimismo, no hay cesión cuando el promotor es responsable y el que trata (equipo investigador). El establecimiento de convenios resulta benéfico en este rubro.

Asimismo señaló que una Comisión técnica es la encargada de implementar las medidas de seguridad con los responsables y usuarios de bases de datos nacionales AFID, ANSES, RENAPER. Por ello, la regulación se adecua a los niveles de acceso, las competencias y funciones, así como los códigos para el acceso a la información.

Para que el tratamiento sea lícito debe estar registrado. El Registro Nacional de bases de datos se estableció para conocer el universo de bases de datos y para que el ciudadano conozca quién y cómo tratan sus datos.

NORA DONATO, DIRECTORA DE ASUNTOS JURÍDICOS DE ADMINISTRACIÓN NACIONAL DE MEDICAMENTOS, ALIMENTOS Y TECNOLOGÍA MÉDICA (ANMAT)

Nora Donato trató el tema del consentimiento informado, mismo que está regulado en la ANMAT N°533097. En ello se contempla la existencia del patrocinante, mismo que puede

ser una persona o institución que inicia un estudio clínico de investigador. Por otra parte, se prevé como participantes a los investigadores de los institutos.

En la Declaración de Helsinki se consagran los principios de confidencialidad: de las personas a las que se les hace estudios o investigaciones. Conforme a este documento, el consentimiento informado debe reunir las siguientes condiciones:

1. Por escrito,
2. Formalmente aprobado,
3. Informado,
4. Previo al ingreso,
5. Voluntario.

En lo que corresponde al expediente clínico, historia clínica o formulario clínico individual, deben tratar datos personales desasociados en lo que corresponde al tratamiento, transferencia, y cuidados sanitarios. Por ello se requiere de estándares mínimos en la seguridad del tratamiento, mecanismos de disociación de datos e informática médica procesos de encriptación.

V. EL REGISTRO NACIONAL DE BANCO DE DATOS PÚBLICOS Y PRIVADOS

Moderador: PABLO SEGURA, COORDINADOR TÉCNICO Y LEGAL DE LA DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

El Ponente abundó en el mecanismo de Internet para la inscripción al Registro Nacional de Banco de datos públicos y privados. Este procedimiento consiste en cargar el formulario www.jus.gov.ar/datospersonales; después de ello, el sistema entrega una remisión de nota con firma certificada y por último, entrega un certificado de inscripción, el cual contiene medidas de seguridad.

El Registro de protección de datos notifica al titular de los datos. En este sentido, se vela por la publicidad de los tratamientos de datos personales existentes para facilitar acceso y corrección.

Las funciones del Registro General de Protección de Datos consiste entre otros en la inscripción de ficheros, autorizaciones de transferencias internacionales, código tipo y catálogo anual de ficheros

Los ficheros públicos que se crean deben publicarse en el Diario Oficial de la Federación respecto de las atribuciones de la oficina gubernamental. Asimismo, es necesario informarse sobre el colectivo de personas sobre los que recae el fichero.

En la hoja de solicitud de inscripción al registro, se debe informar si el fichero es público o privada, si son en soportes papel, magnético o de internet. Asimismo, se notifica el código y antes se usa para futuras modificaciones en el catálogo anual.

Segura destacó que existen años escalonados para el registro de ficheros de acuerdo con las medidas de seguridad. Existen niveles bajo 99, medio 2000 y alto 2001. El registro es declarativo, gratuito de servicio, de concientización y firma electrónica.

La inscripción de los ficheros al Registro es obligatoria y se realiza en dos fases, la primera es para las bases de datos privadas y la segunda para el sector público. Posterior a ello, se les otorga un certificado de inscripción con la categoría de datos.

El ponente hizo alusión de la estadística española, en donde existen 483,079 ficheros. 47,000 son públicos y 435,558 privados. Hasta el momento, existen 59 autorizaciones de transferencias, así como códigos tipo

RAMIRO SORIA, COORDINADOR GENERAL DE SISTEMA DE IDENTIFICACIÓN NACIONAL TRIBUTARIO Y SOCIAL (SINTyS)

El ponente se orientó a señalar la legislación local en las principales medidas adoptadas en la experiencia argentina a efecto de definir niveles de acceso, de lo cual demandó su adecuación.

Según lo dicho por Soria, SINTyS, es un programa gubernamental creado para brindar transparencia en la asignación de beneficios sociales y aumentar la efectividad de las políticas fiscales en Argentina. Su misión es coordinar el intercambio de numerosas bases de datos que existen en los organismos nacionales, provinciales y municipales del país para que la información social y fiscal de la población no resulte fragmentada, desarticulada e inconsistente.

De acuerdo al ponente, el apoyo profesional y tecnológico del SINTyS permite a funcionarios y gobernantes:

- Planificar políticas públicas a información certera
- Focalizar el gasto social y aumentar el cumplimiento tributario
- Lograr una gestión más transparente
- Disminuir los índices de corrupción y mejorar su imagen

La base de datos del SINTyS puede imponer sanciones establecidas en la legislación sobre régimen tributario. Por ello, este sistema, al constituir un registro destinado a dar información, se habilita una vez publicada su reglamentación en el Boletín Oficial.

DR. JULIO PUEYRREDÓN, ABOGADO, SOCIO DE PRICE WATERHOUSE COOPERS

El ponente es de la opinión que desde la óptica de las empresas, las barreras de protección de datos se indagan en razón de lo siguiente: 1. Cumple con las leyes; 2. Políticas; 3.

Seguridad; 4. Acceso, recolección; 5. Calidad de los datos; y 5. Criterios de recolección de la información personal.

DANIEL R. ALTMARK, ABOGADO Y DIRECTOR DEL INSTITUTO DE INFORMÁTICA DEL COLEGIO PÚBLICO DE ABOGADOS DE LA CAPITAL FEDERAL (CPACF)

Altmark considera que tanto los organismos públicos y las empresas tienen la obligación de adecuación de sus operaciones al marco jurídico de la protección de los datos personales; en ese contexto, para el cumplimiento de la normativa existen responsabilidades patrimoniales, penales y, en cascada, una base de solidaridad ilimitada ante la responsabilidad.

Para el ponente fue importante remarcar que nadie puede alegar el desconocimiento de las medidas de seguridad por quién elaboró la base de datos. La calidad de los datos personales empieza con la obtención, por ello es necesario conocer las áreas de impacto de las empresas, la tecnología empleada, clientes, proveedores, terceros, competidores, normas de seguridad, legislación internacional, estándares y políticas del habeas data. Las ventajas de este conociendo radica en los sellos de calidad empresarial y en evitar responsabilidades patrimoniales en cascada por incumplimiento a estas reglas.

ENCUENTRO INTERNACIONAL DE PROTECCIÓN DE DATOS PERSONALES EN LAS TELECOMUNICACIONES

**Buenos Aires, Argentina
28 Y29 de Octubre de 2004**

VI. ASPECTOS TÉCNICOS DE LAS COMUNICACIONES ELECTRÓNICAS PARA NO TÉCNICOS

JUAN CARLOS AQUERRETA, VICEPRESIDENTE DE COMERCIO ELECTRÓNICO Y CONTENIDOS DE CABASE (CÁMARA ARGENTINA DE BASES DE DATOS Y SERVICIOS EN LÍNEA)

La ponencia consistió en el tópico de los factores que condicionan al recorrido físico o “rutas” de los datos. Por ello se propusieron marcos regulatorios en telegramas, presiones comerciales de mercado y las condiciones de operatividad integridad de porciones de la congestión real física. Destaca la regulación de las redes privadas como el intranet, extranet, Internet y los “mirrors”, mismos que sirven para replicar los datos para regiones.

Aquerreta especificó cómo las rutas principales seguidas por el ICANN (Gobierno mundial de Internet), a las PIT-IX que pueden salir al extranjero y a las NAP'S, las cuales se pueden quedar en el país. En este orden de ideas, se destaca que el Internet no es una red absolutamente descontrolada debido a que cada agente tiene un grado de control específico. Europa, Estados Unidos y Chile tienen todos los contenidos. En este sentido, las NAP'S no son únicas, ni permanentes, dependen de las políticas de estado, pueden alterarse y demás.

ING. ARIEL GRAZIER, SECRETARIO DE CABASE, PRESIDENTE DE INTRATEL NETWORKS, PROFESOR ADJUNTO DE LA CÁTEDRA DE COMUNICACIONES II DE LA UNIVERSIDAD TECNOLÓGICA DE ARGENTINA

La Organización Internacional de Estándares (ISO) publicó el modelo de *interconexión de sistemas abiertos* (OSI) en el año de 1984, como respuesta a la entonces incipiente y creciente necesidad de intercambiar información entre sistemas electrónicos heterogéneos, lo cual llevó a la ISO a buscar la manera de regular dicho intercambio de información creando este modelo de comunicaciones.

En palabras de Grazier, El modelo OSI define las reglas para la entrega precisa de los datos en una comunicación electrónica. La división que el modelo OSI realiza de las comunicaciones electrónicas en partes más pequeñas, mejora y facilita la interoperabilidad entre sistemas heterogéneos, concepto básico del modelo dividido en capas, en el cual cada capa esta destinada a ofrecer servicios específicos que interactúan entre sí al momento de establecerse una comunicación electrónica.

Grazier explicó las funciones de las capas que definió el Comité y los servicios que brindan cada una de ellas:

- **NIVEL 7: APLICACIÓN** : Provee servicios generales relacionados con aplicaciones (p.ej.: transmisión de archivos)
- **NIVEL 6: PRESENTACIÓN** : formato de datos (p.ej : ASCII)
- **NIVEL 5: SESIÓN** : Coordina la interacción en la sesión (diálogo) de los usuarios.
- **NIVEL 4: TRANSPORTE** : Provee la transmisión de datos confiable de punto a punto.
- **NIVEL 3: RED** : Define las rutas o caminos de las unidades de información
- **NIVEL 2: ENLACE DE DATOS** : Provee el intercambio de datos entre los dispositivos del mismo medio
- **NIVEL 1: FÍSICO** Define los medios físicos de transmisión como cables y tarjetas de red.

Los niveles de clasificación, criticidad, confidencialidad deben contener al menos la seguridad mínima.

Las políticas generales de estos sistemas se fijan por pautas de revisión establecidas en una sindicatura federal (SIGEN). Destaca el comentario vertido en cuestión de la simulación de páginas *web* de bancos y en consecuencia de los robos, solicitan datos personales con gran precaución.

VII. RETENCIÓN Y PRESERVACIÓN DE DATOS DE TRÁFICO. DATOS DE LOCALIZACIÓN

PHILIP SHOLZ, REPRESENTANTE DEL INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS (IWGDPT)

En opinión de Philip Scholz, los principios para la utilización de datos de localización son la separación de la información de poderes; el secreto en las telecomunicaciones; el diseño minimalista para facilitar su comprensión; el derecho al anonimato, es decir, nadie debe ser forzado a dar sus datos para acceder a Internet; el derecho a la seguridad, es decir, herramientas para asegurar la información personal; restricción secundaria, esto es, un solo fin de uso; transparencia; publicación con amplitud, reglas y normas que existen al respecto, y por último, acceso a datos personales.

GUILLERMO J CERVIO, ABOGADO, SOCIO DEL ESTUDIO BAKER & MCKENZIE

El ponente abundó sobre las disposiciones de la Ley Nacional de Telecomunicaciones, la cual obliga a los prestadores de servicio de telecomunicaciones para informar el origen y destino de telecomunicaciones. Dentro de esa regulación, se define al cliente como el usuario vinculado contractualmente a un prestador. Por otra parte, la norma jurídica mencionada define al usuario como toda persona física o servidores que utilizan los servicios de un prestador.

GABRIELA URQUIDI, DIRECTORA JURÍDICA DE LA SUPERINTENDENCIA DE TELECOMUNICACIONES DE BOLIVIA

La ponente señaló que el uso del Internet y la telefonía móvil posibilitan la apertura de opciones en cuanto al almacenamiento y tratamiento de datos. El marco jurídico en Bolivia en este rubro se remonta a la Ley de Telecomunicaciones N° 1632, la cual prohíbe interceptar, interferir u obstruir el flujo de información en estos medios. No obstante lo anterior, la norma en mención no trata el tema sobre los datos de tráfico, ni su tiempo de almacenamiento de datos de tráfico.

En este sentido, Gabriela Urquidi propone la búsqueda de acciones a futuro para impulsar el desarrollo de las redes y acceso a los servicios sin descuidar las medidas de seguridad y control.

ALBERTO SOTO, ABOGADO E INGENIERO, GERENTE DE TECNOLOGÍA Y COMUNICACIONES DE TECHNYS S. A.

En la perspectiva de Alberto Soto, la retención y preservación de los datos de tráfico radica en el sistema de información empleado. Por ello, el tríptico esencial radica en dos tipos de seguridad, por una parte, la jurídica y por la otra, la de cuestiones tecnológicas de la información.

En este sentido, es necesario ahondar en los antecedentes de retención, quiénes y qué se retiene. Cabe destacar que la composición del sistema de información es *software* y *hardware*, la cual es la estructura de datos personales que tiene conocimiento de todo lo anterior. Desde ese punto de vista, es necesario no atar la legislación a la tecnología.

Respecto al correo electrónico, su protección radica en qué datos debe contener, la identificación del tiempo (día, hora, minuto), de origen (dirección IP). En síntesis, el bien jurídico protegido en los sistemas de información: la información. Cabe señalar que el tríptico esencial consiste en seguridad de la información, es decir, que esta está en el momento en que la necesitas.

Por lo anterior, la ponencia refleja la inquietud sobre qué datos retener por Internet, cuáles son las implicaciones técnico informáticas y las medidas de seguridad. En conclusión, la retención de datos personales de tráfico debe ser en forma consensuada.

MARIA JOSÉ BLANCO ANTÓN, CONSEJERA TÉCNICA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

María Blanco señaló la importancia del marco normativo de la Unión Europea en materia de protección de datos personales, el cual radica en las directivas 1995/46/CE y 2002/58/CE. A su vez señaló que el objetivo principal del paquete Telecom consiste en la protección de libertad y derecho fundamental a la intimidad.

El dato de tráfico se define como cualquier dato tratado a efecto de la conducción de una comunicación a través de la red de comunicaciones electrónicas o a efecto de la misma. Estos datos contienen el número de identificación del abonado, la dirección del abonado, la dirección de tráfico y las garantías en el sistema internacional, cuyo plazo máximo de retención es de 12 meses.

La regla general consiste en la eliminación o preveceía del anonimato y las excepciones a este supuesto son la facturación, promoción comercial y servicio de valor añadido.