Universidad ORT Uruguay

Facultad de Ingeniería

Ley de protección de datos personales

Florencia Sarasola - 126087
Docente: Julio César Fernández

2009

1. Abstract

El 11 de agosto de 2008 en Uruguay se promulgo la ley de Protección de Datos, introduciendo nuevos desafíos, limitaciones y oportunidades. Tanto las bases de datos públicas y privadas cuentan con un periodo de un año para regularizarse.

Posiblemente todas las empresas, organismos y un conjunto significativo de técnicos informáticos se verán afectados por esta nueva normativa. Este articulo pretende ayudarlos a comprender la ley 18.331, su alcance, objetivo y como afecta al ámbito profesional y comercial. También procura esclarecer las acciones que se deben llevar a cabo para el cumplimiento de la normativa.

2. Índice

3. Introducción

El 11 de agosto de 2008 en Uruguay se promulgo la ley de Protección de Datos (ley 18.331). Las bases de datos públicas y privadas cuentan con un periodo de un año para regularizarse (LEY Nº 18.331, 2008).

Posiblemente todas las empresas, organismos y un conjunto significativo de técnicos informáticos se verán afectados por esta nueva normativa. Este articulo pretende ayudarlos a comprender la ley 18.331, su alcance, objetivo y como afecta al ámbito profesional y comercial. También procura esclarecer las acciones que se deben llevar a cabo para el cumplimiento de la normativa.

El cuerpo de este articulo esta diagramado en tres secciones. En el primer capítulo se presentan antecedentes de leyes similares en otros países. En la segunda sección se detalla el contexto que llevo a desarrollar la ley 18.331, sus principales características, las responsabilidades y tareas que habrá que realizar antes del 11 de agosto de 2009. El ultimo capitulo presenta los problemas de implementación y compatibilidad en el ámbito mundial y comercial. Describe las sanciones establecidas en Uruguay y antecedentes en otros países. Incluye también las limitaciones y oportunidades comerciales que supone proporcionar el marco legal que define la ley de Protección de Datos Personales.

4. Referencias

Uruguay mantiene relaciones comerciales principalmente con países miembros del Mercosur, la Unión Europea, el NAFTA (Tratado de Libre Comercio de América del Norte, por su sigla en inglés (North American Free Trade Agreement)) y ALADI (Asociación Latino Americana De Integración). Los principales exponentes comerciales son Brasil y Argentina del Mercosur, de la Unión Europea es España y del NAFTA es Estados Unidos. (CIU (Cámara de Industria y Comercio), 20 Oct 2008)

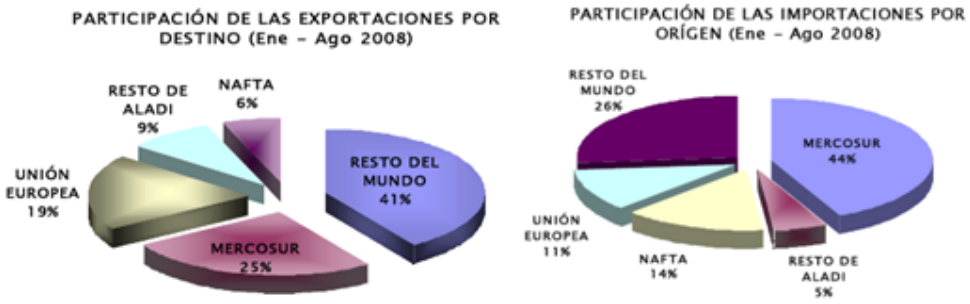

Ilustración 1. (CIU (Cámara de Industria y Comercio), 20 Oct 2008)

Considerando que actualmente la convergencia es un fenomeno observado con particular enfasis en la proteccion de datos, dado que se amplian las posibilidades de transferir datos internacionalmente y que las legislaciones aplican dentro de los limites nacionales (Doneda, Diciembre 2007) y que uno de los motivos que llevaron al desarrollo de la ley 18.331 fue la generacion de nuevas oportunidades comerciales (AGESIC, 2008), se presenta una breve descripcion de la realidad de Brasil, Argentina, Estados Unidos y la Union respecto a la privacidad de datos.

Según Danilo Doneda (2007) y Andrés Guadamuz (2000) existen tres lineas de proteccion de datos personales, las cuales tienen grandes diferencias lo que conyeba a dificultades a nivel comercial. Las lineas son las seguidas por la Union Europea, Estados Unidos y la accion de Habeas Data introducida por Brasil.

4.1 Brasil

En el marco del pasaje a la democracia el Brasil fue el primer país en introducir la acción de Habeas Data en 1988. Esta acción otorga el derecho al individuo de poder acceder así como poder rectificar sus datos almacenados en una base de datos. (Doneda, Diciembre 2007)

En 1997, el Congreso Nacional promulgó la Ley N º 9507, Ley Reguladora del Procedimiento Habeas Data ya que se carecía de directrices adecuadas para la administración de la acción. (Guadamuz, 2000)

A pesar de ser la cuna de la acción de Habeas Data, la legislación brasileña es la menos evolucionada, y una de las herramientas de protección de la privacidad más pobres. La Constitución sólo permite el acceso y la corrección de los datos, no contemplando la actualización y destrucción de los datos. En 1997 se incorpora el derecho de poder añadir una anotación a los datos almacenados en un registro. (Guadamuz, 2000)

4.2 Argentina

Según Pablo Palazzi (Palazzi, 2007), el derecho a la protección de los datos en Argentina radica en brindar el control sobre los datos personales a cada individuo, mediante reglas y principios, el consentimiento para su tratamiento, acciones judiciales, limitaciones a las bases de datos en función de su contenido, en las cesiones o transferencias a terceros y en la intervención de agencias especializadas del Estado destinadas a tutelar estos derechos. Si bien en la reforma de la Constitución Argentina en 1994 se incorporaron los derechos de los titulares de datos frente a los informes comerciales, no fue hasta 2002, que la Dirección de Protección de Datos Personales dictó normas reglamentarias en materia de registro, infracciones, medidas de seguridad y códigos de ética.

Según Andres Guadamuz en 2000 Argentina contaba con la versión de Habeas Data más completa. El artículo 43 de la Constitución, modificado en la reforma de 1994, establece que: “Toda persona deberá presentar el presente recurso para obtener información sobre los datos acerca de sí mismo y su finalidad, registradas en los registros públicos o bases de datos, o en los privados destinados a suministrar información, y en caso de datos falsos o discriminación, esta acción puede ser presentada para solicitar la supresión, rectificación, confidencialidad o actualización de

dichos datos. El carácter secreto de las fuentes de información periodística no se vea perjudicada.”

El sistema argentino de protección de datos personales fue el primero en Latinoamérica en ser reconocido por la comisión de la Unión Europea por su adecuación a la normativa europea en 2003. (Doneda, Diciembre 2007) Sin embargo, el Sr. Palazzi (Palazzi, 2007), señala que para demostrar que se cumple la ley es necesario fortalecer la concientización de los titulares y responsables del tratamiento de datos personales.

4.3 Estados Unidos.

En 1974 se aprobó la ley Privacy Act en Estados Unidos. Esta ley estableció normas para la protección de los datos en poder del Estado. Existieron intentos de extender la protección al sector privado el Congreso no lo permitió. (Hoofnagle, 2006) El foco de esta ley es prevenir el robo de identidad y fraudes. (Johnson, 2007)

En 1976 la Suprema Corte de Estados Unidos sostuvo que los individuos no tienen derecho de privacidad sobre los datos que voluntariamente brindaron a terceros. Esto es lo que se conoce como el “paradigma del secreto” ("secrecy paradigm"), la información es privada si nadie más la conoce. Esto significó que el Estado puede ir a las empresas y solicitarles información personal acerca de sus clientes sin el consentimiento de éstos y sobre todo sin una orden o un pedido judicial que lo autorice. Desde el 11 de Setiembre de 2001, muchas empresas han ofrecido voluntariamente al Gobierno su base de datos con datos personales. (Hoofnagle, 2006)

4.4 Unión Europea

Durante la Segunda Guerra Mundial se obtuvieron y utilizaron datos personales para incrementar la eficacia del Holocausto. (Hoofnagle, 2006) Desde esta base la U.E. (Unión Europea) decreta como derecho fundamental la protección de los datos. La U. E. estableció el primer sistema legal en el mundo que brinda un enfoque global de la privacidad y protección de los datos, abarcando todos los sectores industriales y tipos de procesamiento de datos. (Johnson, 2007)

La diversidad de las razones que motivaron la legislación en la U.E. y EE.UU. hace que las normativas europeas tengan mayor cobertura y sean más restrictivas. La legislación europea utiliza el término “datos personales”, lo que incluye cualquier dato de una persona identificable, por lo que deben ser tomados en cuenta los datos de los empleados, proveedores, usuarios, clientes entre otros. Por otro lado, en Estados Unidos la protección de datos apunta principalmente al consumidor y usuario. (Johnson, 2007)

La U.E. brinda un marco legal, llamado directivas, que obliga a los estados miembros a cumplir. La ley de Protección de Datos de la U.E. se rige principalmente por la Directiva General aprobada el 24 de Octubre de 1995. Dado que las legislaciones de los diferentes países pueden variar, es necesario comprender tanto las directivas como las variaciones de cada miembro. (Johnson, 2007)

5. Legislación de datos personales, Uruguay[1]

5.1 Motivos

Antes de puesta en vigor la ley 18.331, el país contaba con la ley 17.838 para legislar los datos utilizados en informes de carácter comercial, normas constitucionales respecto al secreto de correspondencia y normas legales que abarcan el secreto profesional (art. 302 C. Penal) y secreto bancario (Gonzaga, 2008). La ley de Protección de Datos Personales (LEY Nº 18.331, 2008) incorpora lo expresado por la ley 17.838 y la deroga.

Según lo expresado por la Directora de Área Derechos Ciudadanos de AGESIC (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento) (Viega, 2008) las razones que motivaron la formulación de la ley de Datos Personales fueron:

- Vinculación con terceros países: Se busca el reconocimiento de la Unión Europea como país seguro para el envío de datos personales. Es necesario brindar un nivel adecuado del cumplimiento de las normas, ofrecer apoyo y asistencia a los interesados y proveer de vías de recurso en caso de no cumplirse la normativa y que se vea afectado.

- Captación de inversores: La adecuación a la ley europea permitiría la captación de inversiones en el sector tecnológico y de servicios

- Ofrecer marco regulatorio: El creciente uso de la tecnología de la información y las comunicaciones, ha generado que el tratamiento de datos personales se encuentre en foco para las autoridades nacionales. Debido al valor de las bases de datos personales y al derecho de las personas titulares de los datos de conocer el tratamiento que se les da a sus datos personales y de preservar su privacidad.

El anteproyecto de la ley 18.331 fue elaborado por la AGESIC, incorporando aportes del IDI (Instituto de Derecho Informático, Facultad de Derecho UDELAR) y del Órgano de control del Ministerio de Economía y Finanzas establecido en la ley 17.838. (AGESIC, 2008)

5.2 Propósito

La ley de Protección de Datos Personales tiene como objetivo*"…establecer un marco jurídico claro y necesario para garantizar y hacer efectivo uno de los derechos fundamentales del ser humano, como es el derecho a la protección de los datos de carácter personal y por tanto de la intimidad de las personas."* (Viega, 2008).

[1] A menos que se explicite, toda la información descripta en esta sección se obtuvo de la ley 18.331.

Con la incorporación de esta normativa también se pretende cumplir con los requerimientos de la U.E., para captar empresas europeas que contraten servicios en Uruguay y fomentar la instalación de call centers. (Gonzaga, 2008)

5.3 Alcance

La ley reconocer el derecho fundamental a la protección de datos personales comprendido en el art. 72 de la Constitución. (Art. 1, Ley 18.331) y es de aplicación a personas físicas y jurídicas en cuento corresponda.

El artículo tres establece que "… *será de aplicación a los datos personales registrados en cualquier soporte, que los haga susceptibles de tratamiento…*". Lo que se alinea con la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (Viega, 2008)

Esta ley no aplica a las bases de datos:

- mantenidas por personas físicas para el uso de actividades domesticas o personales
- aquellas cuyo objetivo sea la seguridad publica, defensa, seguridad de Estado y sus actividades en materia penal, investigación y represión del delito.
- creadas y reguladas por leyes especiales

5.4 Terminología

Los conceptos introducidos en esta ley son claves para determinar su alcance e implicancias. Se detallan algunas de las definiciones descritas en el artículo 4. [2]

Dato personal: información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables.
Se consideran datos públicos, los cuales no requieren consentimiento informado a:

- Para personas físicas: nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento.
- Para personas jurídicas: razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.

Dato sensible: datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

Base de datos: conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento electrónico o no, cualquiera que fuere la modalidad de su formación almacenamiento, organización o acceso.

Tratamiento de datos: operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como

[2] Referirse a la ley 18.331 por más información.

también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Titular de los datos: persona cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la ley.

Responsable de la base de datos o del tratamiento: persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.

Encargado del tratamiento: persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento.

Usuario de datos: toda persona, pública o privada, trate datos, ya sea en una base de datos propia o a través de conexión con los mismos.

5.5 Habeas data

La definición manejada por Wikipedia respecto a Habeas data es la siguiente.

Habeas data es una acción constitucional o legal que tiene cualquier persona que figura en un registro o banco de datos, de acceder a tal registro para conocer qué información existe sobre su persona, y de solicitar la corrección de esa información si le causara algún perjuicio.

La ley 18.331 si bien se ajusta a la normativa europea, incorpora también la tercera línea de protección de datos, la acción del Habeas Data (Artículo 37).

Artículo 37 ***Habeas data.-*** *Toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y -en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización- a exigir su rectificación, inclusión, supresión o lo que entienda corresponder.*
Cuando se trate de datos personales cuyo registro esté amparado por una norma legal que consagre el secreto a su respecto, el Juez apreciará el levantamiento del mismo en atención a las circunstancias del caso.

5.6 Responsabilidad legal

La ley establece que todos aquellos que actúen en relación a datos personales de terceros deben cumplir los principios generales de legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva y responsabilidad.

Esto implica que las bases de datos deberán ser inscriptas y su finalidad no podrá violar los derechos humanos ni ser contraria a leyes o la moral pública (Principio de legalidad).

Los datos personales deberán ser veraces, adecuados, ecuánimes y no excesivos en función de la finalidad para la que fueron recabados. Los datos deben ser actualizados de requerirse y si caducan deben ser suprimidos (principio de veracidad).Los datos no podrán utilizarse para una finalidad distinta para la que fueron obtenidos y deberán ser eliminados si ya no son útiles para sus fines (existen excepciones por valor histórico, estadístico o científico, que permite conservar los datos). No podrán comunicarse datos entre bases de datos sin previo consentimiento informado del titular (Principio de finalidad).

Según el Principio de previo consentimiento informado, el titular debe haber prestado si consentimiento libre, previo, expreso e informado el que deberá documentarse para tratar los datos. Quedan exentos de esto los datos públicos y datos:

- De fuentes públicas de información
- Recabados para el ejercicio de funciones del Estado.
- Provengan de una relación contractual, científica o profesional del titular de los datos y sean necesarios para su desarrollo o cumplimiento.
- Para uso exclusivo personal o domestico por personas físicas o jurídicas.

El responsable o usuario de la base de datos debe garantizar la seguridad y confidencialidad de los datos. El artículo 10 prohíbe registrar datos en bases de datos que no reúnan las condiciones técnicas de integridad y seguridad. (Principio de seguridad de los datos)

Quienes hayan obtenido datos de fuentes legítimas están obligados, aun después de terminada la relación con el responsable de la base de datos, a guardar el secreto profesional, usarlos de forma reservada y exclusivamente para las operaciones habituales de su giro o actividad. Esta Ley prohíbe toda difusión de los datos a terceros. (Principio de reserva)

El responsable de la base de datos es el responsable por cualquier violación de la ley 18.331.

Al solicitar información se deberá informar, entre otras cosas, la finalidad de los datos, quienes los utilizaran, el responsable de la base de datos, las consecuencias de brindar o denegar los datos y que el titular puede acceder, rectificar y solicitar la eliminación de sus datos.

El titular de los datos tiene derecho, previo identificación, a obtener toda la información que se halle en una base de datos, tanto pública como privada. Esta información debe ser brindada dentro de los cinco días hábiles luego de solicitada, deberá ser entregada en un formato que permita su entendimiento y no se podrá cobrar por ella. Si el titular solicita la modificación o eliminación de datos, se cuentan con cinco días hábiles para realizar el trámite.

Los datos no podrán ser utilizados para evaluar el rendimiento laboral, la fiabilidad, conducta o cualquier aspecto que pueda afectar al titular de manera significativa.

Respecto a la comunicación de datos, a menos que alguna ley lo permita o que se desasocie la información del titular, se requerirá consentimiento. El destinatario quedara sujeto a las mismas obligaciones legales y reglamentarias del emisor.

En el Capítulo IV – Datos especialmente protegidos de la Ley 18.331 se especifica el trato, obtención, derechos y deberes sobre datos sensibles, relativos a la salud, a telecomunicaciones, a actividades crediticias o comerciales bases de datos con fines de publicidad y datos transferidos internacionalmente, donde se prohíbe la transferencia a un destino que no proporcione niveles adecuados de protección según los estándares del Derecho Internacional o Regional.

Existen un conjunto de circunstancias que permiten la transferencia de datos. Por ejemplo al tratarse de datos médicos, transferencias bancarias, cooperación en la lucha contra el crimen organizado, el terrorismo y el narcotráfico o si el titular lo autorizo.

El articulo 23 concluye: *"… la Unidad Reguladora y de Control de Protección de Datos Personales podrá autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías suficientes respecto a la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos."*

5.7 Órgano regulador

Se creó la Unidad Reguladora y de Control de Datos Personales, como Órgano de Control. El que funciona en forma desconcentrada de la AGESIC.

Los cometidos de esta unidad, respecto a la Ley 18.331 son:

- Asistir y asesorar a las personas.
- Dictar normas y reglamentaciones.
- Realizar un censo de las bases de datos incluidas en la ley de protección de datos.
- Mantener registro de los censos.
- Controlar el cumplimiento de las normas sobre integridad, veracidad y seguridad.
- Solicitar información sobre el tratamiento de los datos.
- Emitir opinión respecto a sanciones administrativas por el incumplimiento de la ley.
- Asesorar al Poder Ejecutivo en proyectos de ley que refieran a la protección de datos personales.
- Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables.

5.8 Registro de datos

Según lo establece el capitulo sexto de la ley 18.331 todas las bases de datos, tanto públicas como privadas deben inscribirse en el Registro que proporciona el Órgano de Control. Para lo que se tiene tiempo hasta el 11 de agosto de 2009.

Para la registración se debe rellenar el formulario correspondiente (órgano público, persona física o jurídica), adjuntando un certificado notarial que garantice el origen de

las firmas del formulario. Los documentos pueden solicitarse al Área de Derechos Ciudadanos de la AGESIC.[3]

La inscripción debe contener la siguiente información:

- Identificación de la base de datos y el responsable de la misma.
- Naturaleza de los datos personales que contiene.
- Procedimientos de obtención y tratamiento de los datos
- Medidas de seguridad y descripción técnica de la base de datos
- Protección de datos personales y ejercicio de derechos
- Destino de los datos y personas físicas o jurídicas a las que pueden ser transmitidos.
- Tiempo de conservación de los datos.
- Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.
- Cantidad de acreedores persona física cuyas obligaciones comerciales superen los 5 años.
- Cantidad de cancelaciones por incumplimiento de la obligación de pago si correspondiera.

6. Efectos a nivel comercial de la legislación de datos.

Los efectos a nivel comercial de las legislaciones de datos son innumerables, periódicamente se encuentran en las noticias juicios por violaciones a este tipo de leyes. Pero las implicancias no descansan en la aplicación local sino que también influyen en la transferencia de información. Por esto se señalan dos eventos de carácter mundial para apreciar las dimensiones de las normativas de datos.

Ya en 2000, Andres Guadamuz comentaba sobre los conflictos ente la Unión Europea y los Estados Unidos con respecto a legislación sobre la protección de datos y su efecto sobre la industria estadounidense de comercio electrónico. La U.E. establece requisitos sobre el destino de los datos, no permitiendo la exportación de datos a países que no posean un nivel adecuado de protección de datos. Luego de varias conversaciones se introdujo en las directivas europeas, que pueden ser destino de transferencia de información aquellas entidades estadounidenses que se certifiquen como "puerto seguro". (Johnson, 2007)

Kuner (2008) analizo el principio de proporcionalidad manejado por el Union Europea respecto a la proteccion de datos advirtiendo a la empresas que pusieran atencion a este principio y su implicancia. Kurner detallo en su trabajo areas de procesamiento de datos donde el riesgo de los problemas juridicos ante la aplicación del principio de proporcionalidad puede ser muy alto, por ejemplo:

- Transferencias de datos a países fuera de la Unión Europea.
- Tratamiento de datos sensibles, incluyendo los datos de menores.

[3] Derechos Ciudadanos, AGESIC. Dirección: Andes 1365, Piso 7, Montevideo, Uruguay. Teléfono: (+598 2)901 2929. Correo electrónico: derechosciudadanos@agesic.gub.uy

- Tratamiento de los datos de los empleados.
- Vigilancia por vídeo.
- El uso de la biométrica.

Se podría decir que el principio de proporcionalidad de las directivas europeas se corresponde con el principio de veracidad de la normativa uruguaya, por lo que las observaciones señaladas por Kurner son validas para empresas orientales.

6.1 Sanciones

6.1.1 Uruguay

Las sanciones recaerán sobre los responsables de las bases de datos o encargados del tratamiento de datos personales. Las medidas que se podrán aplicar ante el incumplimiento de esta ley son:

- Apercibimiento
- Multa de hasta 500.000 unidades indexadas
- Suspensión de la base de datos por un lapso de hasta seis días hábiles.

6.1.2 Antecedentes

Existen numerosos antecedentes en la Unión Europea, Estados Unidos y América sobre sanciones ante el incumplimiento de la ley de privacidad y protección de datos. En esta sección se presentaran unos pocos ejemplos con el fin de mostrar los problemas que se enfrentan las empresas y los titulares de los datos.

En diciembre de 2006, Vodafone fue multado con 76 millones de euros en Grecia. Se alegó que Vodafone no protegió su red permitiéndole a que piratas informáticos realizaran el seguimiento de más de 100 cuentas de teléfonos celulares. El importe de la multa refleja el alto perfil de la naturaleza de los hechos: la piratería informática ocurrió durante los Juegos Olímpicos de 2004 en Atenas, y dentro de las cuentas se encontraba la del Primer Ministro Griego, altos oficiales militares, y periodistas. (Johnson, 2007)

En Alemania una empresa tuvo que retirar todas las cookies de su sitio web, en España se impuso una multa de varios cientos de miles de euros a una productora de televisión que divulgo datos de participantes de un programa de televisión sin el previo consentimiento de los titulares, un tribunal finlandés ordenó encarcelar a varios altos ejecutivos de una empresa de telecomunicaciones por monitorear de forma ilegal los teléfonos de sus empleados, luego fue suspendida la pena. (Johnson, 2007)

La Agencia Española de Protección de Datos ha sancionado a la empresa madrileña CC con una multa de más de 6.000 euros por dejar tirados en una calle de la localidad madrileña de Coslada cartas publicitarias con datos de carácter personal. (Brian Nougreres, 2009)

El periodista Álvaro Alfonso reclamó a la ministra del Interior, Daisy Tourné, acceder a los archivos y “ficheros” del Partido Comunista del Uruguay (PCU) que se encuentran en la Dirección Nacional de Información e Inteligencia (DNII). La ministra le remitió el

informe al Departamento Jurídico de la Asesoría Letrada quienes dictaminaron que “el dueño de la información es esta Secretaría de Estado y por supuesto que no se pueden dar nombre de quienes están ingresados en dichos ficheros a terceros” y que “la filiación política partidaria de una persona es de carácter privado y no puede ser revelada a terceros”. (Periodista reclama a Tourné acceso al archivo del Partido Comunista., 2008)

7. Bibliografía

AGESIC. (2008). *Ley Nº 18.331 de Protección de Datos Personales: Análisis e impacto.* Montevideo: AGESIC.

CIU (Cámada de Industria y Comercio). (20 Oct 2008). *Comportamiento del comercio exterior de bienes del Uruguay.* Montevideo, Uruguay.

Doneda, D. (Diciembre 2007). O habeas data no ordenamento brasileiro e a proteção de dados pessoais: uma integração ausente. *Revista de Derecho Comunicaciones y Nuevas Tecnologías* .

Gonzaga, D. D. (2008). Implicancias Técnicas y de Gestión de la Nueva Ley de Datos Personales. *5a. Academia de Actualización Profesional.* Montevideo: PricewaterhouseCoopers.

Guadamuz, A. (2000). Habeas Data: The Latin-American Response to Data Protection. *Journal of Information, Law & Technology* .

Hoofnagle, C. (04 de 07 de 2006). Interview with Chris Hoofnagle. (D. P. Palazzi, Entrevistador) http://www.habeasdata.org/Interview_with_Chris_Hoofnagle.

Johnson, E. H. (Setiembre de 2007). Data Protection Law in the European Union. *The Federal Lawyer* , 44-48.

Kuner, C. (2008). *EU Data Protection. Proportionality Principle.* The Bureau of National Affairs. Privacy & Security Law Report.

LEY Nº 18.331. (11 de Agosto de 2008). NORMAS DE PROTECCIÓN DE DATOS PERSONALES. *LEY Nº 18.331* . Montevideo, Uruguay.

Palazzi, D. P. (2007). *Informes comerciales.* Buenos Aires: Editorial Astrea.

Viega, D. E. (Marzo de 2008). Iniciativa de Regulación en Protección de Datos Personales. *AGESIC* . Montevideo, Uruguay: http://www.agesic.gub.uy/Sitio/presentaciones.asp.

8. Anexos.

Se adjunta un disco compacto con las fuentes consultadas (no todas has sido citadas en el presente documento) y un formulario de registro de base de datos y el modelo de certificado notarial entregado por personal de AGESIC.