Diálogos
Revista Electrónica de Historia

Escuela de Historia. Universidad de Costa Rica
Vol. 11 No. 1 Febrero - Setiembre 2010
ISSN 1409- 469X

PRIVACIDAD Y PROTECCIÓN DE DATOS: UN ANÁLISIS DE LEGISLACIÓN COMPARADA

Dra. Susan Chen Mok

Director de la Revista: Dr. Juan José Marín Hernández jmarin@fcs.ucr.ac.cr

Editor académico: Dr. Ronny Viales Hurtado ronny.viales@ucr.ac.cr

Editores técnicos: MSc. Anthony Goebel Mc Dermott goebel@racsa.co.cr
M.Sc. Marcela Quirós G. marcela.quiros@ucr.ac.cr

http://historia.fcs.ucr.ac.cr/dialogos.htm

"Diálogos Revista Electrónica de Historia" se publica interrumpidamente desde octubre de 1999.

En la cubierta: Puente de don Federico Sobrado. Tempisque.
Fuente: Álbum Gira Presidencial al Guanacaste. Manuel Gómez Miralles.
Colección del Centro de Investigaciones Históricas de América Central CIHAC.
En la web. http://www.cihac.fcs.ucr.ac.cr/

Diálogos está en los siguientes repositorios:

Dialnet, http://dialnet.unirioja.es/servlet/revista?tipo_busqueda=CODIGO&clave_revista=3325

Latindex http://www.latindex.unam.mx/larga.php?opcion=1&folio=12995 ;

REDALYC http://redalyc.uaemex.mx/src/inicio/FrmBusRevs2.jsp?iEdoRev=2&cvepai=11 ;

LANIC http://lanic.utexas.edu/la/ca/cr/indexesp.html ;

Repositorio de Revistas Universidad de Costa Rica http://www.latindex.ucr.ac.cr/

Directorio y recolector de recursos digitales del Ministerio de Cultura de España http://roai.mcu.es/es/inicio/inicio.cmd

DOJAC Directory of open access & Hybrid journals http://www.doaj.org/doaj?func=byTitle&hybrid=1&query=D

msg02735.html

Asociación para el Fomento de los Estudios Históricos en Centroamérica
http://afehc.apinc.org/index.php?action=fi_aff&id=1774

Universidad de Saskatchewan, Canadá
https://library.usask.ca/ejournals/view/1000000000397982

Monografias
http://www.monografias.com/Links/Historia/more12.shtml

Hispanianova
http://hispanianova.rediris.es/general/enlaces/hn0708.htm

Universidad del Norte, Colombia
http://www.uninorte.edu.co/publicaciones/memorias/enlaces.html

Universidad Autónoma de Barcelona
http://seneca.uab.es/historia/hn0708.htm

Repositorio Invenia - Gestión del Conocimiento
http://www.invenia.es/oai:dialnet.unirioja.es:ART0000086144

Enlace Académico
http://www.enlaceacademico.org/biblioteca/revistas-en-formato-digital-centroamerica/

Electronic Resources
http://sunzi1.lib.hku.hk/ER/detail/hkul/3987318

Revistas académicas en texto completo
http://web.prw.net/~vtorres/

Palabras claves
Privacidad de los datos, seguridad informática, política e información, derecho informático, comercio electrónico, derecho de autor, procesamiento electrónico de datos.

Keywords
Data privacy, computer security, politics and information, computer law, electronic commerce, copyright, electronic data processing.

Fecha de recepción: 15 de mayo 2009 - **Fecha de aceptación:** 6 de abril 2020

Resumen

El trabajo presenta un análisis de la privacidad y protección de datos desde la perspectiva del comercio electrónico. Se presenta los principios y las garantías de protección de datos que deben prevalecer y su aplicación e interpretación en un ambiente de comercio electrónico. Se realiza un análisis comparativo de las normas constitucionales, leyes y proyectos relacionados con la temática de privacidad y protección de datos de seis países latinoamericanos: Chile, Colombia, Costa Rica, Ecuador, México y Perú. Se presenta la jurisprudencia aplicada por la Sala Constitucional costarricense en esta materia. Y por último se realiza un análisis del Proyecto de Ley 15178 Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales de Costa Rica presentando sus aciertos, vacíos y recomendaciones.

Abstract

The work presents an analysis of the privacy and protection of information from the perspective of the electronic commerce. One presents the beginning and the protection guarantees of information that must prevail and his application and interpretation in an environment of electronic commerce. There is realized a comparative analysis of the constitutional procedure, laws and projects related to the subject matter of privacy and protection of information of six Latin-American countries: Chile, Colombia, Costa Rica, Ecuador, Mexico and Peru. One presents the jurisprudence applied by the Constitutional Costa Rican Room in this matter. And finally there fulfils an analysis of the Project of Law 15178 Protection law of the Person Opposite to The Treatment of his Personal Information of Costa Rica presenting his successes, emptinesses.

Susan Chen Mok

Es Directora de la Sede del Pacífico de la Universidad de Costa Rica, desde 2002 hasta 2012. Miembro del Consejo Editorial Intersedes desde el 2001. Doctora en Ciencias de la Administración, Máster en Telemática y Licenciada en Ciencias de la Computación e Informática. Profesora Catedrática de diversos cursos de las carreras: Bachillerato en Informática Empresarial, Dirección de Empresas, Turismo Ecológico. Investigadora en temáticas de computación, derecho informático, educación, pymes y turismo.

PRIVACIDAD Y PROTECCIÓN DE DATOS: UN ANÁLISIS DE LEGISLACIÓN COMPARADA

Dra. Susan Chen Mok

INTRODUCCIÓN

El aspecto de privacidad y, más específicamente, lo relacionado con la protección de datos personales es de gran importancia en el ambiente de comercio electrónico. Esto debido a que en cualquier transacción comercial que el consumidor realiza a través de una página Web, el mecanismo mayormente utilizado es por medio de contratos de adhesión, que se basan en formularios prediseñados por el proveedor, y en los cuales, se solicitan información personal al consumidor.

Por otro lado, cuando el usuario accede a una página Web, simplemente para buscar información de algún asunto que le interese, aunque no compre nada, generalmente, le piden información antes de otorgarle el permiso de ingresar a dicha página.

El usuario entrega información sin saber, ni tampoco es informado para qué ni cómo será utilizada dicha información.

El derecho fundamental de la protección de los datos persigue garantizar a la persona un poder de control sobre cualquier tipo de dato personal, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho afectado[1].

PRINCIPIOS Y GARANTÍAS DE PROTECCIÓN DE LOS DATOS Y EL COMERCIO ELECTRÓNICO

En el tema de la protección de la información personal se reconoce la existencia de una serie de principios generales, garantías y excepciones. Los principios generales son esenciales para garantizar, en forma directa, la adecuada protección de la información personal (y, en algunos casos, los intereses legítimos de personas jurídicas), e indirectamente, para salvaguardar los derechos a la privacidad, al honor, a la reputación, a la libertad de expresión (incluyendo la libertad de prensa), entre otros; mediante la generación de un adecuado marco jurídico en donde puedan hacerse efectivos todos y cada uno de estos derechos y garantías fundamentales del hombre.

De acuerdo con Sarra, los principios generales responden a los siguientes fundamentos:

a) Legitimidad y buena fe: se refiere a que la información personal debe ser procesada en forma legítima y no pueda ser utilizada con fines contrarios a la buena fe.
b) Especificación de la finalidad, racionalidad y duración: se refiere a que el tratamiento de la información debe realizarse con fines determinados, que deben ser explícitos y legítimos; y para su divulgación debe mediar consentimiento del titular. La racionalidad de su utilización implica que los datos deben ser utilizados para los fines para los que fueron recolectados. Además, la información solo deberá ser conservada por un período razonable para la consecución de los fines para los cuales fue recolectada.
c) Pertinencia y exactitud: la información sometida a procesamiento debe ser adecuada, pertinente y no excesiva con relación al ámbito y los fines.
d) No discriminación: se debe evitar el tratamiento de los datos de las personas que pueda converger en actos ilegítimos o discriminatorios. Para esto, se ha establecido la prohibición de compilar datos sensibles que incluyan información sobre el origen racial o étnico, vida sexual, opiniones políticas, religiosas, filosóficas o cualquier otra creencia y la pertenencia a asociaciones, sindicatos, etc. Es decir, cualquier tipo de información que pudiera derivar en actos de discriminación sobre las personas.
e) Confidencialidad y seguridad de la información: se debe garantizar que la información personal, solo será tratada por personas autorizadas, y esta información estará protegida contra destrucción, pérdida, alteración o difusión, accesos no autorizados, utilización fraudulenta, contaminación por virus de computadoras, etc. Para esto, se deberán adoptar las medidas técnicas de seguridad y de organización necesarias para garantizar un adecuado resguardo de los datos.[2]

Para que estos principios puedan ponerse en operación, se deben ofrecer las siguientes garantías, de acuerdo con Sarra[3] (2000), Téllez[4] y LOPD[5]. Se comenta, además, su importancia en el ambiente de comercio electrónico.

a) Derecho de conocimiento: los interesados a los que se soliciten datos personales deberán ser, previamente, informados de modo expreso, preciso e inequívoco:
    1) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información;
    2) de las consecuencias de la obtención de los datos o de la negativa de suministrarlos;
    3) del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas;
    4) de la posibilidad de ejercitar los derechos de acceso, rectificación,

cancelación y oposición;
5) de la identidad y dirección del responsable del tratamiento o de su representantes.

Este derecho de conocimiento es aplicable al comercio electrónico, y aún cuando el consumidor no compre, ni contrate nada y solo haya navegado en la Red, acción que, por sí sola, se considera un acto de comercio o de consumo, tal como lo sería en el comercio tradicional, cuando un consumidor visita diferentes establecimientos comerciales requiriendo información sobre determinados productos con el fin de adoptar una decisión de consumo. Generalmente, para acceder a la información de una página Web, ya sea para comprar o no, se solicita que el usuario dé cierta información personal, pero no se explica para qué lo requiere o si estos datos serán objeto de algún tratamiento, cedidos o vendidos a terceros.

El desarrollo de Internet y del comercio electrónico ha generado una amenaza para la privacidad de los consumidores. Internet permite a los proveedores recolectar, analizar y usar la información con gran facilidad y eficiencia. En muchos casos, sin que el propio consumidor se dé cuenta de ello.

Una transacción por Internet, generalmente, requiere que el consumidor provea de una cantidad de información; normalmente, en el comercio tradicional no se solicita. Además, en Internet es usual el ofrecimiento de servicios gratuitos a cambio de información de los usuarios. Toda esta información es recopilada sin informar al consumidor la utilización que se le va a dar, las medidas de protección que tendrán, ni los derechos que tiene sobre ella (acceso, rectificación, oposición).

También cuando el consumidor navega por Internet, él desconoce que su navegación puede ser grabada por mecanismos de seguimiento. Las compañías de comercio electrónico utilizan numerosos métodos para identificar y efectuar seguimientos de los consumidores en la red. Uno de los métodos más conocidos, actualmente, consiste en la utilización de las denominadas "cookies". Estas consisten en que los sitios donde se visita deja una pista en el disco duro ("cookie") del usuario. Esta pista permite al sitio conocer las veces que el consumidor visita al sitio y hacer un seguimiento de la actividad del consumidor, pudiéndose crear así un perfil de gustos de este. El titular del sitio puede negociar, con determinadas empresas, la transmisión de los datos; que luego, será utilizado en campañas publicitarias dirigidas a seguros potenciales consumidores.

Solo el hecho de grabar pistas en el disco duro del consumidor, ya es una flagrante violación a la privacidad. Aunque el consumidor puede fijar el nivel de seguridad de los "cookies", lo cierto es que, la mayoría de los consumidores,

no tienen conocimiento sobre ellos, por lo tanto, aceptan niveles bajos de protección de "cookies" sin conocer lo que son, ni sus implicaciones.

Por otro lado, muchos sitios Web requieren, para que puedan acceder a ellos, el permiso para grabar "cookies", de lo contrario, no permiten que los consumidores accedan a sus páginas. Al menos, en estos casos, se le está haciendo saber al consumidor la posible grabación de "cookies", y es decisión de él si acepta o no. Pero como se dijo antes, la mayoría de los consumidores desconocen qué son, para qué sirven y sus consecuencias.

El carácter ilícito de esta práctica, reside en la invasión de la esfera personal y, por consiguiente, en la vulneración del derecho a la intimidad de una persona. Además, una vez obtenidos esos datos de forma ilícita, el consumidor no podrá nunca controlar el fin para el que podrían ser utilizados, incluso podrían trascender el simple ámbito publicitario.

La posibilidad de que, una vez conocidas sus preferencias, el sujeto pueda ser objeto de comunicaciones comerciales no solicitadas, ni deseadas agrava dichas conductas. Esto último, lleva a la problemática del "spam" o correo electrónico comercial no solicitado.

La información de las direcciones de correo electrónico puede ser obtenida de muchas formas y permiten al proveedor enviar publicidad y así reclutar nuevos consumidores. La información de las direcciones fue entregada a terceros sin que el consumidor supiera de ello.

b) Derecho a que los datos sean de calidad: los datos que se recolecten deben ser exactos, pertinentes, adecuados y no excesivos, y recolectados para los fines determinados.

En el comercio electrónico, muchas veces, el objetivo consiste en obtener la mayor cantidad posible de información sobre el consumidor, para poder determinar sus intereses y hábitos de consumo, creando verdaderos perfiles humanos, y así poder dirigir una publicidad que difícilmente el consumidor podrá rechazar. Además, esa publicidad es enviada al consumidor sin su consentimiento e irrumpe la privacidad de este cuando se encuentra navegando por Internet.

Los datos que se recolecten, debe ser solo para la identificación del usuario o consumidor, y no debe solicitarse datos que no sean relevantes para la transacción que se está realizando. Además, los datos que se recolecten deben ser exactos, es decir, no contener errores que luego pueda perjudicar al propio consumidor. Dentro de esta exactitud, se considera también que los datos deben ser actuales, pues los datos muy antiguos pueden no reflejar, adecuadamente, la situación del titular y, por tal motivo, deben ser corregidos o eliminados.

La pertinencia de los datos depende del tipo de transacción, en el caso de una compra y venta electrónica, los datos serán los necesarios para realizar

la contratación electrónica. No se deben pedir más datos de los necesarios, ni otros que no interesen para dicha transacción. Solo serán usados para llevar a cabo la compra y venta, y almacenados el tiempo necesario para respaldar la transacción y cualquier reclamo de garantía u otra disconformidad.

Derecho de acceso: las personas tendrán derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

Este derecho es importante en el comercio electrónico, ya que es tanta la información que se intercambia, que puede ocurrir que las propias personas no recuerden o no sepan la información que han autorizado que se recaben de él, ni las condiciones en que lo han hecho, por lo que este derecho les permitirá conocer el flujo de datos que sobre ellas se tiene, y lograr ejercer los derechos de cancelación y oposición, si lo desean. Estos derechos junto al de conocimiento, componen el denominado "habeas data o habeas scriptum" de acuerdo con Del Peso y Ramos6.

El problema del comercio electrónico, es cuando el mismo usuario no tiene control de todos los sitios Web que ha visitado y menos aquellos en donde ha entregado información personal, por lo tanto, es difícil que pueda ejercer un derecho de acceso a sus datos, cuando no se acuerda de los sitios visitados. Los programas navegadores guardan un registro de los sitios visitados, esto podría facilitarle al usuario la memorización de los lugares donde entregó información personal, pero esto solo es posible, si el equipo desde donde accedió a Internet sea de uso personal o restringido.

d) Derecho de rectificación y cancelación: permite que el interesado solicite una modificación en los términos de alteración o ampliación, o una supresión o cancelación de aquellos datos que, referidos a su persona, considere como inexactos o irrelevantes o que requieran actualizarse.

Lograr la rectificación o cancelación de los datos almacenados en un archivo sobre una persona cuando no sean correctos permite evitar una toma de decisión que puede afectarle.

Para ejercer este derecho, el titular de los datos debe conocer el contenido de los datos almacenados sobre él, para poder saber si son correctos o actuales, y en caso contrario, solicitar la rectificación o supresión.

Muchas veces, ocurre que los datos son almacenados por un período largo, en bases de datos de los sistemas de información, y no son actualizados. Es deber del titular, conocer en dónde ha entregado datos, y solicitar la rectificación cuando no sean correctos. Pero, también, es deber del propietario de la base de

datos, eliminar los datos después de un tiempo prudencial, este tiempo debe ser solo lo suficiente para respaldar la transacción comercial de eventuales reclamos.

En el ambiente de comercio electrónico, el deber del titular de conocer dónde ha entregado datos es, a veces, imposible de cumplir, como se vio, anteriormente, o una carga de trabajo que desalentaría el uso de la Red. Por otro lado, el deber del propietario queda a la confianza y buena fe de que lo hará, sin ninguna garantía de su cumplimiento.

e) Derecho de oposición: permite a los interesados a oponerse, al tratamiento de los datos que le conciernen. En este caso, sus datos deben ser dados de baja en el tratamiento, cancelándose las informaciones a su simple solicitud.

Esto se da cuando el titular de los datos, no esté de acuerdo con su procesamiento, o no desee que sus datos sean considerados en el procesamiento, puede presentar su oposición y sus datos deberán ser cancelados.

Para que la oposición se pueda dar, el titular de los datos debe conocer la utilización que se les está dando a ellos, y esto, en el ambiente electrónico, puede ser difícil, puesto que, el titular entrega los datos para la transacción que realiza, pero desconoce la utilización que le puedan dar después. El problema viene por la falta de control que tiene el titular sobre los datos personales que entrega.

En principio, una persona puede oponerse al tratamiento de datos falsos, discriminatorios y sensibles, siempre y cuando conozca del tratamiento.

f) Derecho al consentimiento: En todo procesamiento de datos se requiere que el interesado preste su consentimiento, salvo cuando exista una disposición en contrario.

Otro problema se encuentra en la posibilidad de venta o cesión de la información personal de los consumidores sin el consentimiento de los titulares de la misma.

El problema aquí es cuando no hay control por el titular de sus propios datos. Una vez que los datos han sido entregados, no es posible para el titular saber para qué serán utilizados, solo media la confianza de que el proveedor los utilizará para los fines de la transacción electrónica, pero no hay certeza de que así lo sea. No hay control por el propietario de que sus datos personales serán utilizados correctamente para el fin determinado y que le solicitarán su consentimiento para utilizarlos para otros fines.

Una norma, en este sentido, al menos establecería la obligación de que los datos personales solo pueden ser procesados o cedidos a terceros si el titular ha consentido su procesamiento y lo haya autorizado, y da la posibilidad de recla-

mar cuando este derecho se haya violado.

g) Derecho a fijar el nivel de protección: mediante el derecho de autodeterminación se otorga a la persona la posibilidad de determinar el nivel de protección que desea que se otorgue a los datos que le conciernen. Por otro lado, el responsable del tratamiento de los datos deberá adoptar medidas técnicas y de organización apropiadas para asegurar la protección de los datos contra daños, pérdidas o accesos no autorizados.

Esto permite que, la persona decida el nivel de seguridad que desea para sus datos personales. Sin embargo, esta decisión conlleva el establecimiento de ciertos parámetros de tipo técnico que, generalmente, no lo realiza el propio usuario, sino que es una decisión hecha por un técnico informático o personal afín. Lo cual significa que el nivel de seguridad, al fin y al cabo, no lo define el usuario y debe confiar en la definición del nivel de seguridad que lo realiza una tercera persona (administrador de la Red, proveedor de servicios, etc.).

Por otro lado, en el comercio electrónico, los propios proveedores deberían ofrecer el máximo nivel de seguridad a la información personal que solicitan, para proteger los datos de usos fraudulentos, accesos no autorizados, pérdida, alteración o difusión. Generalmente, en el comercio electrónico, las medidas de seguridad para almacenar los datos personales no son suficientes, y esto hace más vulnerable la intromisión a las bases de datos y la sustracción de datos sensibles.

Una de las razones de esta insuficiencia en el nivel de seguridad sobre la protección de datos, se debe a la ignorancia del proveedor así como del consumidor, los cuales desconocen las grandes posibilidades que existen a nivel tecnológico de que terceros accedan a la información que viaja en la red, o está almacenada en un sitio, y la alteren o utilicen para fines no autorizados, sin que el titular o el proveedor se dé cuenta de ello.

h) Derecho de uso conforme al fin: consiste en que el interesado pueda exigir que su información personal sea destinada para los objetivos específicos por los cuales se proveyó.

Se debe garantizar que la información no será utilizada para otros fines. En el comercio electrónico ocurre que los datos que recopilan del consumidor luego se utilizará para enviarle publicidad no solicitada, o también puede pasar que su información sea vendida o cedida a otras empresas para fines mercadotécnicos.

¿Cuáles son los mecanismos que tiene el consumidor para saber y controlar los datos que entrega en una transacción de comercio electrónico? Y ¿cuáles procedimientos existen para poder reclamar, en el momento en que el consumi-

dor se da cuenta que sus datos están siendo usados para otros fines? Estos problemas requieren soluciones a nivel normativo, que permita exigir el uso de los datos conforme al fin.

Por lo tanto, se debe garantizar al consumidor que sus datos solo serán utilizados para los efectos de concretar la transacción comercial electrónica. Y se debe consultar al consumidor su conformidad para darle cualquier otro uso a sus datos.

i) Derecho para la prohibición de interconexión de archivos: este derecho se refiere a que las distintas bases de datos que contienen información personal no puedan consultarse y/o vincularse indistintamente.

Este derecho, en el ambiente de comercio electrónico, es muy importante, porque puede evitar la interconexión de archivos para la creación de perfiles del usuario, o para conocer con detalle todas las transacciones que realiza o llevar un seguimiento de donde se encuentre ubicado.

La interconexión de bases de datos permite la recopilación masiva, instantánea e indiscriminada de datos sobre una persona desde cualquier parte del mundo. Es fácil incorporar información personal en bases de datos y transferirla a terceros u otras bases de datos ubicadas en cualquier parte del mundo; además, puede ser unida y compilada en segundos para hacer referencia a cualquier aspecto de la persona: datos biográficos, datos de domicilio, datos familiares, datos laborales, información financiera, información médica, información ideológica, información académica, información policíaca, pasatiempos, hábitos, información sobre viajes y comunicaciones, información patrimonial, entre otros.

Es muy fácil que un tercero obtenga excesiva información sobre una persona alrededor del mundo, sin que la misma lo haya autorizado o no se entere de qué está pasando con su información, quién la tiene o para qué la está utilizando.

Derecho a la impugnación de valoraciones basadas sólo en datos procesados automáticamente: este derecho pretende asegurar al interesado que no será sometido a una decisión que pudiera tener efectos jurídicos significativos sobre él, cuando esta hubiere sido adoptada sobre la única base de un tratamiento automatizado de datos y fuera destinada a evaluar determinados aspectos de su personalidad, conducta, fiabilidad, rendimiento laboral, etc. Con este objetivo, se otorga al interesado la posibilidad de impugnar los actos administrativos o cualquier decisión privada que implique una valoración de su comportamiento en las circunstancias aludidas.

En la actualidad, prácticamente, todos los procesos de selección y otorgamiento de beneficios, becas, incentivos, bonos, créditos u cualquier otro

tipo de beneficio, se realizan a través de sistemas de información automatizados. Estos sistemas se alimentan con datos de los solicitantes y mediante una fórmula diseñada, automáticamente, con parámetros establecidos en la programación (que estandarizan una situación) realizan la valoración de cada una de las solicitudes y da un resultado que permite a la administración u otra tomar las decisiones de otorgamiento de los beneficios. Generalmente, esta fórmula se diseña para capturar los valores de los datos con los cuales realiza el cálculo o evaluación correspondiente.

Se debe permitir al consumidor aportar otros elementos que pueden ser considerados para tomar una nueva decisión sin intervención del sistema. Pues, no es posible estandarizar todos los casos, siempre existirán excepciones que se deben considerar de forma separada.

Este derecho permite que el individuo impugne valoraciones realizadas sobre la base de un tratamiento automatizado, también que la persona pueda presentar nuevos datos para su consideración y realizar una nueva valoración.

j) Derecho de indemnización: este derecho se refiere a la facultad que poseen los afectados por infracciones a la normativa de protección de datos, de ser indemnizados.

Esto es importante, porque en el comercio electrónico donde interviene un consumidor, este es la parte más vulnerable que debe ser protegida por el Estado. Cualquier daño que sufra el consumidor, debido a la transacción comercial electrónica, debe ser indemnizado por el proveedor.

En el comercio electrónico, esto se complica en las transacciones que traspasan fronteras. Se deben establecer mecanismos que permitan la indemnización de forma ágil y eficaz para los consumidores.

k) Derecho de tutela: este derecho otorga a las personas la facultad de reclamar ante la autoridad competente, frente a las actuaciones contrarias o que violen sus derechos sobre la protección de sus datos personales.

El Estado debe establecer el organismo competente o los procedimientos adecuados que asegurarán la protección de las personas frente al tratamiento indebido de sus datos personales, o cuando se le deniegue el ejercicio de cualquiera de sus derechos. Se deben establecer mecanismos ágiles y eficientes para los casos en que la violación de los derechos ocurre por un proveedor o empresa no ubicada en el país.

La garantía de ciertos derechos debe proveerla el Estado (tutela, indemnización) para que el consumidor pueda tener acceso al reclamo cuando considere que sus derechos han sido lesionados.

Derecho a la no discriminación: se refiere a que se prohibirá la recolección de datos sensibles que puedan resultar en la discriminación de las personas por su condición, ya sea: social, étnico, sexual, salud, político, religioso, filosófico, gremial, etc.

En el comercio electrónico se debe evitar la recolección de datos sensibles, solo se debe recolectar los datos necesarios para concretar una contratación de compra y venta electrónica.

Es necesario educar al consumidor sobre sus derechos y responsabilidades, para que pueda realizar compras seguras y satisfactorias en Internet, que permita un adecuado equilibrio entre el desarrollo de la economía y su protección como ciudadano. Al hacer un recuento de las actividades que realiza un consumidor para llevar a cabo una transacción de compra y venta electrónica, y considerando el análisis anterior se puede identificar que en una compra y venta por Internet, debe cumplirse lo siguiente, para proteger la privacidad del consumidor:

1- Informar al consumidor, si el sitio que accede está grabando "cookies" en su computador, y las consecuencias de ello. Es decir, informar desde este momento sobre los "cookies" y para qué sirven, y obtener el consentimiento del consumidor.
2- El consumidor debe ser responsable de informarse para fijar el nivel de seguridad adecuado a sus intereses.
3- Informar al consumidor, si el sitio está grabando su información personal electrónica y no electrónica y el uso que se dará a esa información y consultar si está de acuerdo.
4- Informar sobre el nivel de protección que tendrán sus datos, y que estos no serán cedidos, vendidos o transferidos a terceros sin su consentimiento. El nivel de seguridad debe proteger los datos de usos fraudulentos, accesos no autorizados, pérdida, alteración o difusión.
5- En caso de que la transacción comercial sea con una empresa ubicada en el extranjero, informar al consumidor si sus datos serán transferidos a un país con poca protección de datos personales, para obtener su consentimiento para la recolección de datos.
6- Consultar al consumidor, si desea que se le envíe publicidad a su dirección electrónica o cuando se encuentra navegando por Internet.
7- Informar los derechos que tiene el consumidor sobre sus datos, si puede consultarlos, rectificarlos, oponerse a su procesamiento, o acceder a ellos en cualquier momento.
8- Los datos que se recolecten debe ser exactos, pertinentes, adecuados, no excesivos, y utilizados conforme al fin establecido (para la transacción

de compra y venta electrónica), y se mantendrá por un período finito (lo necesario para respaldar la realización de la compra y venta electrónica y los casos de cumplimiento de garantías).

9- Prohibir que se interconecten archivos para procesar datos de un consumidor para obtener perfiles de sus actividades, sin su consentimiento expreso.
10- Prohibir la recolección de datos sensibles que puedan después utilizarse para negar una venta o un servicio al consumidor, o tratarlo de manera diferente.
11- Permitir que el consumidor impugne una valoración que se ha tomado con base solo a los datos procesados automáticamente. Y valorar su condición tomando en consideración otros datos aportados por él que pueden cambiar su valoración inicial.
12- El Estado debe garantizar la tutela de las personas a la protección de sus datos personales y, en consecuencia, también los derechos del consumidor a la protección de sus datos personales. Y la indemnización de las personas cuando sus derechos han sido lesionados.
13- El Estado debe informar y educar a las personas para que puedan establecer relaciones de consumo responsable (tome sus propias medidas de seguridad, conozca lo que ocurre en la red, sea cauto al realizar una transacción comercial electrónica, se cerciore para qué le piden datos personales y los derechos que tiene sobre ellos, y sobre todo, que conozca los procedimientos para reclamar cuando sus derechos le sean violados).

ANÁLISIS DE LEGISLACIÓN COMPARADA: CHILE, COLOMBIA, COSTA RICA, ECUADOR, MÉXICO, PERÚ.

Los países latinoamericanos han establecido la protección a la vida privada como un derecho de rango constitucional a partir del cual se han iniciado la redacción de los proyectos de leyes específicas que regulan dicha materia.

Normas Constitucionales

En la Constitución Política de Chile no existe una norma expresa, pero la construcción jurídica de la protección de datos personales se basa en el artículo 19 n° 4, inciso primero, de la Constitución Política de la República, que reza:

CAPITULO III. De los Derechos y Deberes Constitucionales
Artículo 19.- La Constitución asegura a todas las personas: (…)
4º.- El respeto y protección a la vida privada y a la honra de la persona y de su familia.[7]

En la Constitución Política de Colombia, se encuentra el artículo 15 que establece el derecho de las personas a la intimidad personal y familiar y al buen nom-

bre, e indica que el Estado debe respetarlos y hacerlos respetar. También, establece el derecho 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.

El artículo dispone que, en la recolección, tratamiento y circulación de datos, se respete la libertad y demás garantías consagradas en la Constitución.

También establece que las formas de comunicación privada son inviolables, excepto por orden judicial para los casos que la ley establezca.

La Carta Constitucional costarricense no contempla, específicamente, el derecho a la protección de datos de carácter personal, como un derecho específico a ser tutelado. Pero, su artículo 24, establece la protección en el ámbito de intimidad del hogar, de las comunicaciones y de los documentos privados, dejando a la ley la regulación de las interceptaciones telefónicas y el secuestro de documentos. Indica que, los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República son inviolables.

Se encuentran, en la Constitución Política de Ecuador, los siguientes derechos tutelados:

El inciso 8, del artículo 23, de la Constitución, garantiza la intimidad personal y familiar; inciso 13, la inviolabilidad y el secreto de la correspondencia; inciso 21 del mismo artículo, prohíbe la utilización de la información personal de terceros referentes a sus creencias religiosas, filiación política, datos sobre salud y vida sexual.

El artículo 94, de la Constitución de 1998, de Ecuador, establece la tutela por medio del hábeas data:

> Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito.
> Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos.
> Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización.
> La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional.[8]

En México, el artículo 16, de la Constitución de los Estados Unidos Mexicanos, señala que, nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones. Del mismo modo, regula casos relativos a la práctica de cateos, visitas domiciliarias, la exhibición de documentos y papeles personales, así como la violación de correspondencia. Las disposiciones señaladas no se refieren, específicamente, a la regulación de los datos personales propiamente, sino al derecho a la privacidad.

La Constitución Política de Perú de 1993, en el artículo 2°, inciso 6) esta-

blece el derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. A su vez el artículo 200º inciso 3) de la Constitución Política de 1993, establece la Garantía Constitucional del "Hábeas Data" (Ley Nº 26301 modificada por la Ley Nº 26545, y la Ley Nº 23506), que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2º, incisos 5, 6 y 7 de la Constitución.

El artículo 2°, inciso 5, que norma, por primera vez, el derecho a solicitar de cualquier entidad pública, sin expresar la causa, la información que requiera y a recibirla, salvo que esa información afecte la intimidad personal, o aquellas que, expresamente, se excluyan por ley o por razones de seguridad nacional.

Así el derecho a la información ante una entidad pública encuentra como uno de sus límites a la intimidad personal. A su vez, la misma norma constitucional protege el secreto bancario y la reserva tributaria, los cuales solo pueden levantarse a pedido del juez, del Fiscal de la Nación, o de una comisión investigadora del congreso con arreglo a ley y siempre que se refieran al caso investigado.

El inciso 7) del mismo artículo, reconoce los derechos a la intimidad, al honor y a la propia imagen; y por último, el inciso 10) del referido artículo 2°, consagra también la reserva e inviolabilidad de las comunicaciones y documentos privados, los cuales no pueden ser abiertos, interceptados, intervenidos ni incautados, solo por mandato motivado del Juez, con las garantías previstas en la Ley.

Leyes generales o en proyecto

Chile fue el primer país de Iberoamérica que aprobó la ley de protección a la privacidad, que contiene varios principios fundamentales sobre protección de datos personales.

La ley chilena 19628, sobre la protección de la vida privada, indica en su artículo 4 que el tratamiento de los datos personales solo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta, expresamente, en ello. Y que el titular de los datos debe ser, debidamente informado respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.

También, este artículo 4, legaliza el "spam" o correo comercial no solicitado al indicar que:

> No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.[9].

Su artículo 6 indica que:

> los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos.[10]

El artículo 16 de esta ley establece el recurso del "hábeas data", aunque no se refiere a este término explícitamente.

Colombia no tiene una norma general de Protección a la Vida Privada. Ecuador no tiene una norma general de Protección a la Vida Privada; sin embargo, en la Ley 67 de Comercio electrónico, firmas y mensajes de datos establece en su artículo 9:

> Art. .9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.
> La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.
>
> No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.
>
> El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.[11]

Igualmente, México no tiene una norma general de protección a la vida privada. Sino que, mediante el artículo 76 bis de la Ley Federal de Protección al Consumidor amplía el alcance de la Ley en transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados.

Esta Ley mexicana es la primera en Latinoamérica en referirse a la protección de datos personales en sistemas y servicios en línea, pero legisla sólo en este tipo de transacciones. Además, adopta un enfoque basado en la protección al consumidor, cuando pueden existir situaciones donde la recopilación y tratamiento de información no provenga de una relación con el consumidor, por lo que hay un vacío jurídico que persiste[12].

Perú no tiene una norma general de protección a la vida privada, pero se encuentra en el Código Civil lo siguiente:

> Artículo 16.- Confidencialidad de la correspondencia y demás comunicaciones.
> La correspondencia epistolar, las comunicaciones de cualquier género o las grabaciones de la voz, cuando tengan carácter confidencial o se refieran a la intimidad de la vida personal

> y familiar, no pueden ser interceptadas o divulgadas sin el asentimiento del autor y, en su caso, del destinatario. La publicación de las memorias personales o familiares, en iguales circunstancias, requiere la autorización del autor.[13]

Podría considerarse aquí, que los datos recopilados en las contrataciones por medios electrónicos, son parte de una comunicación y, por lo tanto, amparado por el Código Civil.

Ecuador, Perú, Colombia, México y Costa Rica no tienen ninguna ley general de protección de datos personales. Sin embargo, Perú, Colombia, México y Costa Rica han presentado proyectos a discusión:

Colombia tiene en estudio el proyecto de ley estatutaria N° 143 de 2003, por la cual se dictan disposiciones para la protección de datos personales y se regula la actividad de recolección, tratamiento y circulación de los mismos. Y tiene otro Proyecto de Ley Estatutaria 071-2005, del 10 de agosto de 2005, por la cual se dictan las disposiciones generales del "hábeas data" y se regula el manejo de la información contenida en bases de datos personales, en especial, la financiera y crediticia, y se dictan otras disposiciones.

Costa Rica tiene el Proyecto de Ley No.15.178 Protección de la persona frente al tratamiento de sus datos personales. El texto pasó a Comisión Permanente de Asuntos Jurídicos de la Asamblea Legislativa el 27 de marzo de 2003.

También tiene otro proyecto de Ley No.14785 que adiciona un nuevo capítulo denominado Del Recurso de "Habeas Data" al Título III de la Ley 7135, de Jurisdicción Constitucional, este proyecto pasó a estudio de la Comisión Permanente de Asuntos Jurídicos el 18 de junio de 2002.

Por otro lado, está el Proyecto de Ley No.14029 de Acceso a Internet, con dictamen afirmativo de mayoría de la Comisión Permanente de Asuntos Económicos del 15 de mayo de 2001, establece en su artículo 6, inciso g) que los proveedores de servicios de Internet no pueden ceder los datos personales a terceros sin autorización del titular; y su inciso b) establece la inviolabilidad de las comunicaciones y documentos privados por Internet.

Aunque Costa Rica no tenga una Ley propiamente relacionada con la Protección de Datos, el acceso no autorizado a datos personales o privados contenidos en medios electrónicos, informáticos, magnéticos y telemáticos tiene protección en el Código Penal costarricense, y en otras normas específicas como la Ley General de Aduanas, la Ley de Administración Financiera de la República y Presupuestos Públicos, el Código de Normas y Procedimientos Tributario, entre otras.

Se encuentra en el Código Penal costarricense, el artículo 196 bis, que establece la violación de comunicaciones electrónica como un delito. Este artículo establece penas de seis meses a dos años al que vulnere la intimidad de otro. Es decir que, sin su consentimiento se apodere, accede, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino mensajes,

datos e imágenes contenidas en medios electrónicos, informáticos, magnéticos y telemáticos. Las penas serán de uno a tres años, si estas acciones son realizadas por los propios encargados de los soportes electrónicos, informáticos, magnéticos y telemáticos en donde se encuentra almacenado los datos.

Los artículos 217 bis y 229 bis del Código Penal, se refieren al fraude informático y al sabotaje informático, respectivamente, los cuales consisten en acceso, modificación o daño a los datos contenidos en los sistemas informáticos. Estos artículos establecen penas de uno a diez años de prisión.

México tiene presentado el Proyecto de decreto de Ley Federal de Protección de Datos personales desde el 2001, y en su capítulo VI establece lo relacionado al "Hábeas Data".

Perú tiene un anteproyecto de ley de Protección de Datos Personales elaborado por la comisión especial constituida por el Poder Ejecutivo mediante la Resolución Ministerial N° 094-2002-JUS, está todavía en trámite.

La Sala Constitucional costarricense y la protección de datos

Como se puede observar del análisis de las secciones anteriores, Costa Rica no cuenta ni con una ley de protección de datos personales, ni con el recurso de "Hábeas Data" expresamente en su normativa.

Sin embargo, el "hábeas data" se ha convertido en un instrumento de tutela reactivo que ha sido ampliamente aplicado por Sala Constitucional costarricense, tomando como base la misma Ley de la Jurisdicción Constitucional, así como la interpretación amplia que la propia Sala ha hecho del artículo 24 de la Constitución Política.

La jurisprudencia de la Sala Constitucional ha evolucionado notablemente, los primeros fallos se establecen en contra de los archivos criminales administrados por el Organismo de Investigación Judicial (voto 2609-91, 2680-94 mencionado en Chirino y Carvajal[14]. En una de las primeras sentencias, se considera el suministro de informaciones conservados en esos archivos a terceras personas (desviación del fin original del tratamiento de datos) como lesivo al principio de legalidad y a la dignidad de la persona.

La sentencia 1261-90 reconoce el derecho a la intimidad y el derecho a acceder al amparo para protegerlo. En esta sentencia, la Sala anuló por inconstitucional la posibilidad de intervenir, inclusive con fines de investigación policial, las líneas telefónicas[15].

También en la sentencia 9080-94, Barth[16] indica que la Sala Constitucional avaló la negativa de la institución aseguradora de vehículos de mostrar los datos declarados por quien sufrió una colisión, inclusive a la parte contraria en el mismo accidente automovilístico. La sentencia declaró el carácter confidencial de esos datos resguardados por el asegurador.

La sentencia 4147-97 (reiterada en la sentencia 4154-97), la Sala acogió el recurso de amparo planteado por quien exigió del patrono que le mostrara el expediente personal, abierto durante el proceso de reclutamiento de personal. En esta sentencia, el tribunal afirma un principio esencial en el derecho de la autodeterminación informativa: el derecho al acceso a los datos personales acopiados en una investigación.

Posteriormente, y ya en el orden de fallos más reciente, el Voto 4154-97, habla expresamente del "hábeas data" y su regulación, planteando que el objeto de este recurso es la protección de la persona para conocer o rectificar la información pública o privada que exista sobre ella. En este sentido, se encuentra en Chirino y Carvajal lo siguiente:

> La Sala Constitucional ha reconocido la existencia de un amparo especial, denominado "hábeas data" cuyo objetivo esencial consiste en el ejercicio de una facultad de corrección de los datos que se hallan en bancos de datos públicos y privados.
> La primera sentencia que alusión (sic) a este tema es la número 4154-97. Califica al hábeas data, correctamente, como una institución de carácter procesal, cuya tutela se extiende a bienes jurídicos tales como el honor, la intimidad y la dignidad de la persona.[17]

La Sala Constitucional reconoce los peligros de la sociedad informatizada con el fallo 1345-98, de acuerdo con Chirino y Carvajal:

> Fue el primer fallo donde se establece una relación inequívoca entre los peligros de la "sociedad informatizada" y el derecho a la intimidad.
>
> Hace un reconocimiento de los riesgos que las tecnologías de la comunicación y la información podrían traer para la sociedad y el ciudadano, sobre todo en lo referido al acceso a los datos personales[18]
> Los magistrados constitucionales hacen evidente que "…esfera privada ya no se puede reducir al domicilio o a las comunicaciones sino que es factible preguntarse si debe incluir "la protección de la información" para reconocerle al ciudadano una tutela a la intimidad que implique la posibilidad de controlar la información que lo pueda afectar.[19]

Esta sentencia, indica Barth[20], marca un hito en materia del derecho a la autodeterminación informativa. El problema sometido al conocimiento del Tribunal se desencadenó, porque una empresa suministró a un banco información sobre una persona, contra la cual existía, según la empresa, una deuda incobrable. En realidad, la deuda estaba prescrita y el recurrente así exigía que se aclarara en la base de datos. En igual sentido, se dirige la sentencia 8996-2002.

En el expediente 15178, del proyecto de ley de Protección de la persona frente al tratamiento de datos personales, menciona que el Voto 1345-99, abre la posibilidad de una tutela de acceso, con base en el derecho a la autodeterminación informativa, para que la gente pueda conocer las informaciones que sobre ellas se encuentren registradas, e incluye una descripción de los derechos que lo asisten.

En un fallo más sistematizado, el 5802-99, la Sala Constitucional entra a analizar el registro y los bancos de datos y los objetivos del "hábeas data", así como los principios que rigen el ejercicio de estos derechos. En esta sentencia, la Sala se pronuncia en cuanto al deber de excluir del archivo policial las reseñas de personas absueltas o sobreseídas, definitivamente, en un proceso penal. Indica la Sala que "Mantener su ficha en el archivo no solo roza con el derecho a la autodeterminación informativa, sino también con el principio de inocencia"[21]

Indica Chirino y Carvajal[22] que este fue el primer fallo donde la Sala abordó los principios que regulan el tratamiento de datos personales, y dio cabida a que el ciudadano pueda controlar la forma en que se realiza el tratamiento de datos personales, dentro de la tutela procesal del "hábeas data".

Las siguientes sentencias de la Sala son mencionadas en Barth[23]. La sentencia 6481-99, la Sala considera también confidenciales los datos presentados por un tercero en la oferta dentro de una licitación pública, y rechaza la petición de tener acceso a ellos.

La sentencia 2885-2002 obligó a la empresa excluir de sus archivos datos sobre los parientes de quien solicita el crédito, pues esto se desvía de la finalidad del archivo.

En la sentencia 2002-6783, la Sala obligó a una empresa que aclarara la identidad de una persona cuyos datos constaban en el archivo. El problema surgió porque la empresa de datos suministra a un banco el historial crediticio de una persona, pero al no constar ningún número de identificación, y por existir la posibilidad de personas con igual nombre, no es posible determinar, exactamente, si se trata de quien gestiona el crédito. Igual sentido se pronunció la Sala en sentencia 2002-10438.

La sentencia 2000-3820, declaró con lugar un recurso de amparo a favor de un periodista que reclamaba tener acceso a los pasaportes diplomáticos de varios funcionarios del servicio exterior. El acceso debe darse no solo a los periodistas, sino a toda persona que lo solicitara. En este mismo sentido, se pronuncia la Sala en la sentencia 2002-4802 en relación con la lista de personas autorizadas por el Ministerio de Obras Públicas y Transportes para brindar el servicio de transporte público; y la sentencia 2003-3489 que obliga a un banco estatal, en aras de la transparencia, a revelar la información de las cuentas corrientes que tienen a su nombre los distintos partidos políticos y las sociedades anónimas que utilizaron para canalizar los fondos de la campaña electoral.

Se observa que, la Sala ha desarrollado varios principios esenciales en torno al derecho a la protección de datos personales: el derecho a la intimidad y a la protección de datos personales, a la tutela de ese derecho por la vía del recurso de amparo, derecho a exigir la exclusión del registro de información contenidos en archivos, derecho a la confidencialidad, derecho al acceso a sus datos personales,

el derecho a la actualización de los datos, derecho a la exclusión de información sensible y el derecho a una adecuada identificación de la persona cuyos datos se almacenan. También la Sala ha establecido excepciones de dar información personal a terceras personas.

Este recuento de la jurisprudencia de la Sala Constitucional, en materia de protección de datos, permite observar el avance que ha tenido la jurisprudencia nacional en materia de "hábeas data", como un estándar de tutela reactivo de indudable importancia. No obstante, al igual que en otros países, aún es necesario acordar tutelas preventivas, que reaccionen antes de que se ocasionen riesgos de incalculables proporciones para una gran cantidad de ciudadanos, sobre todo, en la nueva era de la sociedad de la información y del conocimiento.

Hoy resulta indispensable ofrecer al país una regulación integral que ofrezca mecanismos preventivos que considere el desarrollo tecnológico, para completar la tutela reactiva que ya ofrece el máximo tribunal constitucional.

Análisis del Proyecto de Ley 15178 Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales de Costa Rica

El actual proyecto parte de la premisa de que la vía del "hábeas data" ya ha sido, adecuadamente, aplicada por la Sala Constitucional, y ya ha ido ampliándose su uso, incluso, para establecer ciertos elementos de calidad en el tratamiento de datos. Resulta evidente, entonces, que debe incluirse en una legislación una consideración amplia de las etapas del tratamiento de la información que forman parte normal de todos los procesos informativos en el ámbito público y privado, incluyendo, el flujo transfronterizos de datos.

Del análisis del Proyecto de ley 15178 se observa que este no incluye dos derechos: Derecho para la prohibición de interconexión de archivos y el Derecho a la impugnación de valoraciones basadas solo en datos procesados automáticamente.

Sería conveniente adicionar ambos derechos, pues el primero se refiere a que no se permite interconectar diferentes archivos para procesar datos personales con el fin de crear perfiles de gustos, preferencias o de simple consumo, de la persona. Recuérdese que, con la tecnología actual, es muy fácil y veloz conocer todo acerca de una persona con solo procesar los datos que de ella se encuentran en distintas bases de datos. Se debe prohibir, a los responsables de los datos, la transmisión o cesión de datos personales a terceros, que podrían utilizarlos con fines no autorizados; además, no debe permitirse que se interconecten archivos para cruzar información de las personas.

También, es necesario incluir el derecho a la impugnación de valoraciones basadas solo en datos procesados automáticamente, porque el procesamiento automático de datos personales no garantiza que se consideren todos los elementos

importantes de una persona para valorar o tomar una decisión sobre ella. Recuérdese que el procesamiento automático tiene parámetros definidos para evaluar alguna situación de la persona, pero no todas las situaciones de la personas son iguales, y más de alguna requeriría de tratamiento diferenciado por sus condiciones personales.

El primer capítulo, se refiere al objeto y fin del proyecto de Ley, así como una lista de definiciones de algunos de los conceptos contenidos en su articulado.

Establece que, el objetivo de la ley es garantizar a cualquier persona física o jurídica, sean cuales fueren su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida privada y demás derechos de la personalidad; asimismo, la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

No establece el ámbito de aplicación como un artículo aparte. Sería conveniente incluirlo para especificarlo. Se recomienda seguir la Directiva 95/46/CE la cual establece que las disposiciones de la Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

El capítulo II, del Proyecto de Ley, establece los principios básicos para la protección de datos, regulando los aspectos relacionados con el derecho de las personas respecto del manejo de sus datos, reconociendo los deberes de obtención del consentimiento del afectado, calidad, seguridad y cesión de los datos, categorías de datos que requieren de una protección mayor a la regla general (datos sensibles), garantías efectivas de acceso a la información personal, corrección, supresión y actualización de la misma. También, prevé la posibilidad de las entidades de emitir protocolos de actuación.

Con respecto a la seguridad, el artículo 7, establece, en su inciso 2, que el responsable del fichero deberá adoptar las medidas de índole técnica y organizativa necesarias, para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado; también, el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

El inciso 3 indica que, no se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones para garantizar plenamente, su seguridad e integridad y los de los centros de tratamientos, equipos, sistemas y programas.

El inciso 4 establece que, por vía de reglamento, se establecerán los requisitos y las condiciones que deban reunir los ficheros automatizados y los manuales y las personas que intervengan en el acopio, almacenamiento y uso de los datos.

Por último, el inciso 5, obliga al secreto profesional al personal que intervenga en cualquier fase del proceso de recolección y tratamiento de los datos de carácter personal.

El artículo solo se refiere a la seguridad de los datos almacenados en los ficheros automatizados y manuales, debe indicarse, también, la seguridad de los datos en tránsito a través de los medios electrónicos de comunicación.

Con respecto a la seguridad de los datos personales transmitidos a través de la red, esta se logra por medio del sistema de Criptografía asimétrica, con autoridades certificantes y firmas digitales. Pero, la seguridad en los lugares de recepción, procesamiento y almacenamiento de la información debe incluir entre otros: políticas empresariales o institucionales sobre medidas de seguridad, protocolos de seguridad, auditorías, controles, mecanismos tecnológicos para su resguardo (claves para los responsables), así como medidas de protección contra daños fortuitos (incendio, humedad, etc.).

Es importante que, se establezca, explícitamente, la obligación de que las empresas, que manejan datos de las personas, tengan todas las medidas adicionales de seguridad necesarias para la protección adecuada de los datos de las personas.

Con relación a la cesión de datos, indica, el artículo 6, que los datos de carácter personal conservados en archivos o bases de datos públicos o privados, solo podrán ser cedidos a terceros, para fines, directamente, relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del afectado, y el consentimiento no será exigido, cuando así lo disponga una ley o se trate de la cesión de datos personales al Estado o una institución pública de salud o de investigación científica en el área de la salud, relativos a la salud, y sea necesario, por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados.

Se resalta sobre la importancia de la disociación, pues, inclusive, en el caso de que sea el Estado el que requiera los datos personales, para cumplir con sus fines, es necesario que, los datos no puedan asociarse a persona determinada.

Sobre los protocolos de actuación, se resalta el artículo 13, el cual establece la posibilidad de que las personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, almacenamiento y uso de datos personales, de emitir un protocolo de actuación, en el cual establecerán los pasos que deberán seguir, en la recolección, almacenamiento y manejo de los datos personales, de conformidad con las reglas previstas en la Ley.

Estos protocolos deben ser inscritos ante el Registro de archivos y bases de datos y aprobados por la Agencia de Protección de Datos Personales, la cual podrá verificar que el titular del archivo esté cumpliendo con los términos de su código de conducta. Estos protocolos permitirán que las entidades actúen de manera ágil y sencilla, en tanto se sometan a los términos de sus propios protocolos.

Estos protocolos de actuación o código de conducta son mecanismos de autorregulación. Sin embargo, este artículo solo establece la posibilidad de emitir

el protocolo de actuación. Sería importante incluir, a nivel de ley, que el Estado incentivará la adopción de mecanismos de autorregulación, para promover que las empresas implementen estos mecanismos para la protección de la privacidad y del tratamiento de datos personales.

El capítulo III, del Proyecto, establece como regla general, la prohibición de la transferencia internacional de datos. Su único artículo 14, establece que las personas públicas y privadas encargadas del manejo de bases de datos y los archivos físicos, estarán imposibilitadas para transferir datos que hayan recibido, directamente, de los titulares de la información o de terceros, pero se exceptúan de esta prohibición las transferencias que cumplan las siguientes reglas:

> **a)** Que la Agencia para la Protección de Datos Personales autorice la transferencia a la persona o institución receptora, pública o privada, por corroborar que con dicho traslado no están siendo vulnerados los principios rectores del manejo de datos personales, descritos en esta Ley.
>
> **b)** Que el titular de la información haya autorizado expresa y válidamente tal transferencia.
>
> **c)** Si se trata de una persona o institución pública o privada domiciliada en el extranjero, dicha transferencia solo podrá ser llevada a cabo si, además de las condiciones antes mencionadas, dicho receptor está domiciliado o tiene como base un país que ofrezca un nivel de protección de los datos personales, igual o superior al establecido en Costa Rica.[24]

Este artículo es importante para los casos de transacciones comerciales electrónicas que traspasan fronteras. Por lo tanto no se podrá transmitir datos a países que tengan un nivel inferior de protección de datos que al establecido en Costa Rica. Con esta norma, se pretende prevenir la violación a las reglas sobre manejo de datos personales producida por su indebida cesión a personas domiciliadas en países que cuentan con una pobre protección de datos personales. Con esta norma, Costa Rica estaría regulando la materia en forma similar a la prevista en la normativa producida por la Unión Europea (Directiva 95/46/CE).

Pero, a diferencia de la Directiva Europea, el Proyecto no incluye, las mismas excepciones, por las cuales se ha permitido las transferencias de datos personales a países que no ofrecen protección adecuada. Excepción que, ha permitido a las compañías acogerse a cláusulas contractuales tipo o crear sus normas corporativas vinculantes y aceptadas por la Unión Europea, como instrumento para garantizar la protección de datos, cuando el país no las ofrece.

Sería conveniente, incorporar la posibilidad de que, en caso de que el país, a donde se transferirá los datos personales, no ofrezca protección adecuada, se permita la transferencia utilizando instrumentos como las normas corporativas vinculantes, los contratos con cláusulas tipo (utilizadas en la Unión Europea), u otros acuerdos similares al de Puerto Seguro, que garanticen dicha protección. Esto

con el fin de no limitar las relaciones comerciales, siempre y cuando se realicen con una protección adecuada de los datos personales transferidos.

Otro aspecto importante, del Proyecto de Ley, es que crea y define en su capítulo IV, la Agencia para la Protección de Datos Personales (PRODAT), dándole a esta la autoridad para velar por el cumplimiento de la Ley y sancionar a los que la incumplan, además, es la encargada de llevar el control de todos los archivos, registros o bases de datos, públicos y privados, existentes sobre datos personales. Con este órgano dotado de independencia funcional, administrativa y de criterio, se intenta dar una efectiva garantía de los derechos derivados del manejo de datos personales, pues exime a los órganos jurisdiccionales, del conocimiento de los procesos de "hábeas data" tradicional. Sus funciones propuestas son tanto preventivas (inscripción y autorización de las bases de datos y protocolos de actuación, inspecciones oficiosas, etc.), como reactiva (atención de denuncias, imposición de órdenes y sanciones administrativas, etc.).

El capítulo V, se regulan los procedimientos de intervención en archivos y bases de datos, el régimen disciplinario aplicable a los administradores de ficheros y los procedimientos internos, para ejercer la competencia disciplinaria contra los funcionarios de la Agencia.

El Proyecto de Ley, no incluye, explícitamente, el procedimiento por seguir en caso de violación a un derecho cometido por algún ente, público o privado, ubicado en el extranjero. El proyecto solo establece normas para aplicarse a nivel nacional y solo el artículo 14, se refiere a la prohibición de la transferencia de datos a otros países con niveles inferiores de protección. Pero, por ejemplo, cuando un proveedor vende a través de Internet y recolecta información de un consumidor nacional, no hay mecanismos para realizar un reclamo ágil y efectivo si el proveedor viola algún derecho del consumidor en relación con sus datos personales. Por lo tanto, debe agregarse en el Capítulo de Procedimientos del Proyecto de Ley, el detalle de cómo se abordaría en caso de que el denunciado sea alguien ubicado en el extranjero. Es importante indicar que, en casos de que estas violaciones se den en las relaciones de consumo, la jurisdicción aplicable sea la del domicilio del consumidor.

La aprobación del Proyecto de Ley 15178, sería un avance importante porque permitiría proteger los datos personales de todos los ciudadanos, y en especial, al consumidor, cuando este los entrega al proveedor en sus relaciones de consumo electrónico.

En un sentido más amplio, es necesario establecer la normativa de privacidad y protección de datos personales, de lo contrario, Costa Rica podría verse como un paraíso del tráfico de datos personales y podría verse afectada en sus pretensiones de mercado global, en los actuales momentos, cuando el país está negociando diferentes tratados de libre comercio con Estados Unidos, la Unión Europea

y países asiáticos.

A la par de este proyecto, debe también aprobarse el proyecto de adicionar el recurso de "hábeas data" expresamente a la Ley de Jurisdicción Constitucional costarricense, para garantizar el ejercicio del derecho de la persona a acceder a las informaciones personales que se encuentren disponibles en registros magnéticos y manuales con el fin de ser revisados, y si representan para la persona un perjuicio, también el de ser corregidos o eliminados. Aunque, la Sala Constitucional ya reconozca el "hábeas data", como se analizó en la sección correspondiente.

Como lo indica Chirino y Carvajal:

> Alcanzar altos estándares en esta materia significa además, una ineludible condición para participar en las negociaciones comerciales con mercados altamente sensibles a nuestros productos, como son los de la Unión Europea, cuyas directivas y normativas exigen que los países con los cuales se tengan relaciones de este tipo demuestren que tienen estándares similares de protección a los ofrecidos en los países miembros.[26]

CONCLUSIONES Y RECOMENDACIONES

Para que haya un desarrollo más rápido del comercio electrónico, se requiere la confianza del consumidor. Para esto, las empresas de bienes y servicios deben labrarse una reputación que respalde y dé seguridad a todas sus transacciones electrónicas, principalmente, las realizadas a través de Internet, que permitan una mayor confianza de la población consumidora, para hacer compras por medio de sus páginas Web. Además, es necesaria una base legal que proteja, adecuadamente, la información personal y vida privada de los ciudadanos.

Es necesaria una combinación de ambos mecanismos, autorregulación y base legal, que permita una adecuada protección a la vida privada y al tratamiento de la información personal. Concluye Reindenberg[27] que los ciudadanos que deseen participar en el mundo digital necesitan la seguridad de que su información personal será tratada adecuadamente. Y las empresas que realizan comercio electrónico no pueden fallar en el uso adecuado de los datos personales.

La protección de la privacidad y el tratamiento de la información personal no pueden dejarse a la libre, esperando y confiando que las empresas se autorregulen, o dejarse completamente al Estado, para que emita la normativa necesaria. El desarrollo vertiginoso de la tecnología, requiere una mezcla complementaria de ambas partes, Estado y empresas e industrias privadas, que permitan ofrecer al consumidor una adecuada protección de su intimidad y, a la vez, promuevan el desarrollo del comercio electrónico.

Por otro lado, como lo expresa Arias[28], el país no puede pasar ningún proyecto de ley relacionado con elementos que giren alrededor de las tecnologías

digitales, si antes no se dicta y aprueba una ley, que proteja a cada uno de los nacionales de los excesos en el tráfico y manejo de sus datos.

Los países europeos iniciaron el camino de la regulación con legislaciones de protección de datos, después vino la legislación en comercio electrónico, firmas digitales, etc. En Costa Rica, está ocurriendo lo contrario, ya se ha promulgado una ley sobre firmas y certificados digitales y documentos electrónicos; pero, todavía no cuenta con una, para la protección de datos personales. Habría que ver lo que ocurrirá en los próximos años, en materia de protección de datos personales, a raíz del vertiginoso desarrollo del comercio electrónico.

Retomando la situación de los países latinoamericanos analizados, se encuentra que Chile tiene una Ley vigente de Protección a la Vida Privada en la cual se incluye el recurso del "hábeas data", un avance importante en la normativa chilena. Sin embargo, no establece un órgano fiscalizador independiente que se encargue de velar por el cumplimiento de las disposiciones de esta Ley, por lo cual adolecerá de una efectiva ejecución. Esta Ley chilena, tampoco establece nada al respecto de la transferencia internacional de datos, lo cual permite concluir que se encuentra permitida, siempre y cuando se cumplan las disposiciones generales establecidas en la Ley.

De acuerdo con Palazzi[29], la ley chilena cumple parcialmente los recaudos exigidos por Europa para considerar adecuada una legislación o un sistema de privacidad. Esto debido a que varios principios de protección requeridos por la Unión Europea no están presentes en la ley chilena, falta normas que prohíban las transferencias a terceros países y la carencia de una autoridad de aplicación que vigile el efectivo cumplimiento de las normas.

En materia de comunicaciones comerciales y mercadeo directo, Chile legalizó el envío de correos electrónicos no solicitados o "spam", pero permite los titulares de datos personales ejercer el derecho de bloqueo y eliminación de los datos personales almacenados en una base de datos; de manera que, el responsable del banco de datos no pueda continuar enviando comunicaciones comerciales y correos electrónicos no solicitados a quien ha ejercido este derecho.

En otras legislaciones, como la Ley 34/2002, sobre telecomunicaciones y servicios de la sociedad de la información y del comercio electrónico de España, en materia de comunicaciones comerciales y correos electrónicos no deseados se ha optado por la prohibición de enviar comunicaciones comerciales y correos electrónicos no deseados a las personas (artículo 21), salvo que, las mismas hayan autorizado con anterioridad el envío de dichas comunicaciones y correos (artículo 22).

El problema del "spam" hace que muchos consumidores se vean forzados a cambiar de correo electrónico, además el "spam" tiene un costo económico para los proveedores de servicio de Internet, y para el consumidor que paga por tiempo real de uso de su conexión a Internet.

Chile, Perú y México incluyen, en sus leyes de protección al consumidor, artículos relacionados a la publicidad enviada por correo electrónico, permitiendo al consumidor solicitar suspender estos envíos.

Ecuador no tiene una ley propiamente de protección a los datos personales, pero incluyó en la Ley 67 de Comercio electrónico, firmas y mensajes de datos un artículo de Protección de Datos.

México tampoco tiene una ley de protección a la privacidad, pero en su Ley Federal de Protección al Consumidor se refiere a la protección de datos en transacciones en líneas para relaciones establecidas con consumidores.

Colombia, Ecuador y Perú incluyen dentro de su norma Constitucional el recurso de "Hábeas Data". En el caso de Chile, el "hábeas data" se encuentra en el artículo 16 de la ley chilena 19628, sobre la protección de la vida privada.

En el caso de Costa Rica, aunque expresamente no se tiene el recurso de "hábeas data", la Sala Constitucional lo ha reconocido y lo ha aplicado en diversas sentencias que ha dictado, como se analizó en la sección correspondiente.

Sin embargo, el "hábeas data", ya sea como acción constitucional o reglamentada, a través de una ley, no alcanza a cubrir todos los problemas de la protección de datos y tiene solo la posibilidad de solucionar algunos de los problemas ocasionados por las nuevas tecnologías de la información.

Como indica Argüello[30], el "hábeas data" incluye solo los derechos de acceso y rectificación, y de acuerdo con Chirino y Carvajal[31], es un tipo de tutela reactiva, porque el ciudadano puede accederla, cuando el daño ya ha ocurrido.

Esto indica que es necesaria la promulgación de leyes de protección de datos personales, si se quiere proteger, efectivamente, los derechos de las personas a su intimidad, en esta nueva era de las tecnologías de información y comunicación.

Mientras, no se aprueben en esos países leyes de protección de datos siguiendo los estándares europeos, no existirá una autoridad de control encargada de velar por un correcto y adecuado tratamiento de datos personales junto con un código que condense estos principios. Aunque Perú, Costa Rica, México y Colombia no tienen todavía una ley de Protección de datos personales, o en general, a la Protección de la Vida Privada, es un acierto que ya hayan presentado proyectos en este sentido para su discusión.

En el caso de Costa Rica, la norma constitucional (art. 24) garantiza la privacidad y el derecho a la intimidad, que debe ser respetada a nivel de las relaciones comerciales. Además, Costa Rica firmó la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica) el 22 de noviembre de 1969, cuyo artículo 11, inciso 2 establece: "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación."

Como se dijo, Costa Rica no tiene todavía una ley de Protección de la Vida Privada, sin embargo, el hecho de que en la Constitución lo establezca como un derecho fundamental, hace obligatorio su cumplimiento.

Se considera un avance el hecho de que ya haya un proyecto en este sentido presentado a la Asamblea Legislativa. Este proyecto de Ley de Protección de la persona frente al tratamiento de sus datos personales es muy completo en términos de aplicación de los principios de tutela y de la creación de una organización técnica específica dirigida a ser un modelo institucional de tutela.

Considerando las garantías revisadas, el proyecto de ley costarricense no establece nada sobre las siguientes garantías:

Derecho para la prohibición de interconexión de archivos, Derecho a la impugnación de valoraciones basadas sólo en datos procesados automáticamente.

Por tanto, se recomienda incorporar en el proyecto estas garantías.

Tampoco establece nada respecto a las "cookies" y a la distribución de direcciones electrónicas a terceros para asuntos mercadotécnicos, sin el consentimiento del titular de la dirección, aunque esto último puede decirse que el Reglamento autónomo de servicio para la regulación del correo electrónico masivo no deseado de RACSA, viene a solventar esta situación, una medida interesante de analizar, puesto que RACSA, es el proveedor del servicio de Internet, no así el responsable directo de la publicidad enviada. Esto funciona en Costa Rica, pues solo son dos proveedores de servicios de Internet y ambos son del Estado. Sin embargo, en una apertura comercial del país, se debe establecer los mecanismos y las regulaciones a este tipo de actividades.

También es importante incorporar, expresamente, en la normativa sobre protección al consumidor o en la Ley de Protección de la Persona Frente al tratamiento de sus Datos Personales, lo relativo a las "cookies", la distribución no autorizada de direcciones electrónicas a terceros sin el consentimiento del titular y la prohibición del "spam" excepto cuando el consumidor lo autorice.

Se recomienda incluir, en la normativa relacionada con la protección al consumidor, lo relacionado a la protección de datos personales, de manera semejante como lo ha hecho Ecuador, incluyendo un artículo de Protección de Datos en la Ley 67 de Comercio electrónico, firmas y mensajes de datos. Esto debido a que, en una relación de compra venta, siempre el consumidor debe proporcionar datos personales, cuyo tratamiento debe quedar debidamente normado. Esta protección debe incluir la garantía del proveedor de respetar el derecho a la privacidad y a la protección de los datos del consumidor en el ámbito informático, que incluya los siguientes derechos: conocimiento, calidad, acceso, rectificación, oposición, consentimiento, fijar el nivel de protección, uso conforme al fin, tutela, indemnización, no discriminación, prohibición de interconexión de archivos, e impugnación de valoraciones basadas solo en datos procesados automáticamente.

Además, ser recomienda dar trámite más expedito al proyecto de Ley No.15.178 Protección de la persona frente al tratamiento de sus datos personales, el 27 de marzo de 2003, pasó a estudio de la Comisión Permanente de Asuntos Jurídicos y al proyecto 14785, para adicionar el recurso de "Hábeas Data" a la Ley de Jurisdicción Constitucional, que pasó a estudio de la Comisión Permanente de Asuntos Jurídicos, el 18 de junio del 2002, este último para explicitar el recurso en la ley de Jurisdicción Constitucional.

Se detecta el vacío de que el proyecto de ley Protección de la persona frente al tratamiento de datos personales se refiere a la protección del ciudadano en territorio nacional y frente a empresas establecidas en territorio nacional. Si la violación de las garantías establecidas en la Ley es por parte de una empresa o persona en el extranjero, el proyecto de Ley no establece los procedimientos para que el consumidor o ciudadano pueda plantear el reclamo, y que este sea resuelto de forma ágil y eficaz.

Ciertamente, es difícil exigir a las empresas que venden a través de Internet, el respeto a las leyes costarricenses. Sin embargo, la tutela del consumidor es a través de su propio actuar, un consumidor bien informado puede denunciar las violaciones a sus derechos e iniciar los procesos para demandar su indemnización. Se recomienda que el Estado informe y eduque a los consumidores en materia derechos y deberes en el ámbito del comercio y, principalmente, en materia de comercio electrónico.

Por otro lado, se puede afirmar que, la mayoría de los sitios que recolectan información personal de los consumidores, no tienen una política de privacidad o esta es insuficiente. Es decir, no se indica a los usuarios las medidas utilizadas para proteger la información almacenada, cómo y a quiénes se comunicarán sus datos y cómo puede el consumidor acceder a ellos.

Se recomienda incluir en la normativa de Protección al Consumidor la obligación a los proveedores, que recolecten información de los consumidores, tener políticas de privacidad. Que estas políticas se exhiban en forma clara y destacada en la página principal del sitio y, en cada parte del mismo, en que se recolecte información personal, y además debe ser clara, precisa y entendible.

Se propone que, la política de privacidad, incluya lo siguiente:

-la identificación de la empresa dueña y administradora del sitio
-la naturaleza de la información recolectada
-la justificación del almacenamiento de la información
-el uso que se le va a dar
-quiénes comparten la información recolectada
-los derechos de oposición que tiene el usuario
-el tiempo que la información es almacenada
-los mecanismos de seguridad para evitar intromisiones en el almace-

namiento de la información personal, y durante la transmisión por las redes de comunicación
-cómo puede cambiar en el futuro la política de privacidad del sitio
-la identificación de la persona responsable de la privacidad de la información
-la identificación del organismo encargado de vigilar y fiscalizar en materia de tratamiento de datos personales.

Por otro lado, la seguridad en los datos personales, transmitidos a través de la red, se logra por medio del sistema de Criptografía asimétrica, con autoridades certificantes y firmas digitales. Pero, la seguridad en los lugares de recepción y almacenamiento de la información, debe incluir entre otros: políticas empresariales o institucionales sobre medidas de seguridad, protocolos de seguridad, auditorías, controles, mecanismos tecnológicos para su resguardo (claves para los responsables), así como medidas de protección contra daños fortuitos (incendio, humedad, etc.). Debe quedar establecida en la Ley de Protección de la persona frente al tratamiento de sus datos personales, la obligación de las empresas, que manejan datos de las personas, de tener todas estas medidas adicionales de seguridad.

En relación con la transferencia internacional de datos, la aplicación estricta de la Directiva Europea sobre protección de datos puede interrumpir y perjudicar cualquier tipo de transacción comercial que incluya el uso y transferencia internacional de datos personales, el cual se ve potenciado por el desarrollo del comercio electrónico. Cualquier comerciante en línea que está haciendo negocios en Europa, estará sujeto a las normas de protección de datos que esta establece, esto lo obliga a tomar las medidas necesarias para proteger la privacidad de los individuos en relación al procesamiento y difusión de datos personales y la confidencialidad de esos datos.

La Unión Europea solo requiere que los países tengan legislación "adecuada", no que adopten, esencialmente, la misma legislación. La Unión Europea creó un Grupo de Trabajo para examinar las condiciones en los terceros países donde, eventualmente, podrían realizarse transferencias. Además la Unión Europea se encuentra en constantes negociaciones para llegar a un acuerdo y para el caso de empresas individuales, existen vías alternativas en la Directiva para permitir las transferencias a pesar de la existencia de una prohibición general, tal es el caso de contratos o las excepciones.

En Europa no se escatiman esfuerzos dirigidos a conjugar la protección de los datos personales de los individuos de los Estados miembros con los intereses económicos que se derivan de la libre contratación internacional.

De la experiencia europea, se recomienda incorporar, en el proyecto de Ley de Protección de la persona frente al tratamiento de sus datos personales la posibi-

lidad de transferir datos a terceros países que no ofrecen nivel adecuado de protección, siempre que los responsables del tratamiento cumplan con ciertas condiciones que pueden establecerse en instrumentos similares al acuerdo de Puerto Seguro, las Cláusulas Contractuales Tipo o a las Normas Corporativas Vinculantes de la Unión Europea.

Como se vio, la protección de los datos personales es una materia en el cual deben participar el Estado con sus normas y las empresas con formas de autorregulación. Por esta razón, se considera importante no solo posibilitar los mecanismos de autorregulación, sino que se incentive su utilización, y así dejarlo establecido en el Proyecto de Ley costarricense.

Como Costa Rica no tiene aún la Ley, se recomienda realizar las modificaciones para incorporar las observaciones planteadas al proyecto de ley de Protección de la persona frente al tratamiento de sus datos personales y dar trámite más expedito para su aprobación, incluido el proyecto de incorporar el hábeas data a la Ley de Jurisdicción Constitucional. Y de acuerdo con Chirino y Carvajal (2003):

> No puede el país continuar careciendo de una adecuada y detallada regulación referente al manejo de los datos de las personas. No puede seguir dependiendo casi exclusivamente de la jurisprudencia constitucional y de algunas escasas conminaciones penales como únicos mecanismos de tutela de la intimidad. No puede conformarse con algunos mecanismos de tutela reactiva ante las violaciones a la autodeterminación informativa, ni puede seguir teniendo como único órgano protector una instancia jurisdiccional genérica, saturada, y poco dotada de los recursos y conocimientos técnicos necesarios para garantizar una efectiva protección.[32]

Por otro lado, el problema de la tutela de la intimidad, en un ambiente de comercio electrónico, va más allá de la protección a nivel nacional, debido a la necesidad, facilidad y velocidad de las comunicaciones internacionales para establecer las relaciones comerciales u otras relaciones. Por tal motivo, los mecanismos de protección, leyes y otros, deben considerar esta característica de internacionalidad, y por lo tanto, las soluciones no pueden venir a nivel de un país, sino que debe pensarse en grupos de países con los que se permita establecer las relaciones. Si estas relaciones pueden establecerse con cualquier país del mundo, la solución debe ser a nivel de todo el mundo, en este caso, puede ser por medio de los Organismos Internacionales existentes, como: la ONU, la OMC, la OCDE u otros.

Por lo anterior, se recomienda estudiar los mecanismos que ha utilizado la Unión Europea para que el grupo de países que lo conforman respeten y hagan cumplir las directivas sobre protección de datos personales o de la vida privada establecidas a nivel comunitario.

En los casos de archivos, en manos privadas, debe encontrarse mecanismos de protección de las personas, por el uso de sus datos privados semejante al establecido por la Unión Europea para la protección de los datos personales que consten

en los archivos de cualquier institución u organismo de la Comunidad, creando el Supervisor Europeo de Protección de Datos.

Esto último es una propuesta que ya otros autores lo han mencionado, como Palazzi que manifiesta:

> Tal vez la única solución posible en materia de protección de datos personales sea alcanzar un acuerdo mundial, ya sea a través de normas similares, leyes tipo, convenios internacionales, o –como está ocurriendo a la fecha-, con la diseminación del modelo europeo en América Latina, Europa del Este y algunos países de Asia.
>
> La privacidad constituye un valor importante para el desarrollo de una sociedad más democrática, fundada en el respeto de los derechos del hombre. La protección de datos personales es la herramienta destinada a hacerla efectiva en este tema tan sensible de la sociedad de la información.[33]

También Argüello[34] indica que los problemas globales requieren soluciones globales y propone una Red de Protección de Datos Personales a nivel Iberoamericano, propuesta que también la hace Iriarte[35]. Y Aced[36] visiona que lo mejor en un futuro sería llegar a la aprobación de un instrumento internacional vinculante en materia de protección de datos, con vocación universal, que permita el establecimiento de un marco jurídico seguro y estable que sin duda redundará en un incremento de la confianza de los ciudadanos y en un desarrollo más armónico de la Sociedad de la Información.

Se recomienda la promulgación de la normativa de protección de datos personales para los países que todavía no la tienen, en la cual se incluya la creación de Agencias de Protección de Datos. Estas Agencias de Protección de Datos deben ser implementadas a nivel gubernamental de más alto nivel de acuerdo con Iriarte[37], que velen por la adecuada protección de los datos personales, y crear una red regional, mejor aún una red global, que coordine los esfuerzos de estas agencias nacionales con capacidad para perseguir a los infractores de esta ley, de forma ágil, en cualquier parte de la región o del mundo en donde se encuentre.

CITAS Y NOTAS

1 Barriuso, C. 2002. *La contratación electrónica*. 2 ed. Madrid: Ed. Dykinson. P. 425.

2 Sarra, A.V. 2000. *Comercio electrónico y derecho: aspectos jurídicos de los negocios en Internet.* 1. ed. Buenos Aires, Argentina: Astrea.

Sarra (2001)

3 Sarra, A.V. 2000. *Comercio electrónico y derecho: aspectos jurídicos de los negocios…*

4 Téllez, J. 2004. *Derecho Informático*. 3 ed. México: McGraw Hill/Interamericana Editores S.A.

5 *Ley Orgánica 15/99 de protección de datos de carácter personal (LOPD)*. 13 diciembre 1999. B.O.E. 14-12.99. España. Consultado el 26 de marzo de 2009. En: http://protecciondedatos.urjc.es/PD/legislacion/index.php

6 Del Peso, E. y Ramos, M. 1994 *Confidencialidad y seguridad de la información: La LORTAD*

y sus implicaciones socioeconómicas…

7 *Constitución Política de Chile*. 2005. Chile. P. 12. Consultado el 18 de octubre de 2008 en http://www.bcn.cl/pags/legislacion/leyes/constitucion_politica.htm

8 *Constitución Política de Ecuador*. (1998).P. 17. Consultado el 18 de octubre de 2008 en http://www.presidencia.gov.ec/modulos.asp?id=109

9 *Ley19628 Sobre Protección de la Vida Privada o Protección de Datos de Carácter Personal.* Publicada en el Diario Oficial de 28 de agosto de 1999. Chile. P. 4. Consultado el 21 de marzo de 2009 en http://www.informatica-juridica.com/anexos/anexo137.asp

10 *Ley19628 Sobre Protección de la Vida Privada o Protección de Datos de Carácter Personal…*

11 Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos.17 de abril de 2002. Ecuador. http://www.corpece.org.ec/. P. 2. Consultado el 21 marzo 2009.

12 Palazzi, P. 2002. *La transmisión internacional de datos personales y la protección de la privacidad.* Argentina: AD-HOC S.R.L.

13 *Decreto Legislativo 295 Código Civil*. Publicado 25.07.84. Perú. Consultado el 8 de setiembre de 2008 en http://www.cajpe.org.pe/rij/bases/legisla/peru/codciv.htm

14 Chirino, A., Carvajal, M. 2003. *El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica*. Revista Costarricense de Derecho Constitucional. Tomo IV. Costa Rica: Investigaciones Jurídicas S.A. Julio del 2003.

15 Barth, J. F. 2005. *Marco Normativo y Jurisprudencial de la Protección de Datos en Costa Rica.* II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch.

16 Barth, J. F. 2005. *Marco Normativo y Jurisprudencial de la Protección….*

17 Chirino, A., Carvajal, M. 2003. *El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica*. Revista Costarricense de Derecho Constitucional. Tomo IV. Costa Rica: Investigaciones Jurídicas S.A. Julio del 2003. P. 244

18 Chirino, A., Carvajal, M. 2003. *El camino hacia la regulación normativa del tratamiento de….* P. 240

19 Chirino, A., Carvajal, M. 2003. *El camino hacia la regulación normativa del tratamiento de….* P. 241

20 Barth, J. F. 2005. *Marco Normativo y Jurisprudencial de la Protección….*

21 Barth, J. F. 2005. *Marco Normativo y Jurisprudencial de la Protección*….P. 265.

22 Chirino, A., Carvajal, M. 2003. *El camino hacia la regulación normativa del tratamiento de datos personales…*

23 Barth, J. F. 2005. *Marco Normativo y Jurisprudencial de la Protección….*

24 *Proyecto de ley 15178 de Protección de la persona frente al tratamiento de datos personales.* Asamblea Legislativa. Costa Rica. 2003. P. 19. **En:** http://www.asamblea.go.cr/proyecto/15100/15178.doc.**Consultado el 4 de febrero de 2009.**

25 Chirino, A., Carvajal, M. 2003. *El camino hacia la regulación normativa del tratamiento de datos personales….* P.283

26 Chirino, A., Carvajal, M. 2003. *El camino hacia la regulación normativa del tratamiento de datos personales….* P. 284

27 Reidenberg, J. 1999. *Privacidad y comercio electrónico en los Estados Unidos.* Consultado el 20 de febrero de 2009 en http://reidenberg.home.sprynet.com/Privacidad-USA.htm

28 Arias, B. 2002. *Vacíos legales en Costa Rica por el uso de la Red: El "e-practice".* Revista de Ciencias Jurídicas. No. 97. San José: Colegio de Abogados y Facultad de Derecho de la Universidad de Costa Rica.

29 Palazzi, P. 2002. *La transmisión internacional de datos personales y la protección de la privacidad.* Argentina: AD-HOC S.R.L.

30 Argüello, F. 2005. *Protección de datos personales: la directiva comunitaria, su influencia y repercusiones en Latinoamérica.* II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch. P.69-104.

31 Chirino, A., Carvajal, M. 2003. *El camino hacia la regulación normativa del tratamiento de…*

32 Chirino, A., Carvajal, M. 2003. *El camino hacia la regulación normativa del tratamiento de datos personales….*P. 283.

33 Palazzi, P. 2002. *La transmisión internacional de datos personales y la protección…* P. 204.

34 Argüello, F. 2005. *Protección de datos personales: la directiva comunitaria, su influencia y repercusiones en Latinoamérica.* II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch.

35 Iriarte, E. 2005. *Estado situacional y perspectiva del derecho informático en América Latina y el Caribe*. CEPAL. Naciones Unidas. Consultado el 28 de agosto de 2008 en: http://www.cepal.org/publicaciones/DesarrolloProductivo/5/LCW25/LCW25.pdf

36 Aced, E. 2005. *Transferencias Internacionales de Datos. Protección de Datos de Carácter Personal en Ibeoramérica*. II Encuentro Iberoamericano de Protección de Datos. La Antigua-Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch.

37 Iriarte, E. 2005. *Estado situacional y perspectiva del derecho informático en América Latina y el Caribe…*

BIBLIOGRAFÍA

Aced, E. (2005). *Transferencias Internacionales de Datos. Protección de Datos de Carácter Personal en Ibeoramérica*. II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch. P.105-127.

Argüello, F. (2005). *Protección de datos personales: la directiva comunitaria, su influencia y repercusiones en Latinoamérica.* II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch. P.69-104.

Arias, B. (2002). *Vacíos legales en Costa Rica por el uso de la Red: El "e-practice"*. Revista de Ciencias Jurídicas. No. 97. San José: Colegio de Abogados y Facultad de Derecho de la Universidad de Costa Rica.

Barth, J. F. (2005). *Marco Normativo y Jurisprudencial de la Protección de Datos en Costa Rica.* II Encuentro Iberoamericano de Protección de Datos. La Antigua-Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch. P.261-270.

Barriuso Ruiz, C. (2002). *La contratación electrónica*. 2 ed. Madrid: Ed. Dykinson.

Chirino, A., Carvajal, M. (2003). *El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica*. Revista Costarricense de Derecho Constitucional. Tomo IV. Costa Rica: Investigaciones Jurídicas S.A. Julio del 2003. p.195-287.

Del Peso Navarro, Emilio; Ramos González, Miguel Ángel. (1994) *Confidencialidad y seguridad de la información: La LORTAD y sus implicaciones socioeconómicas.* Madrid: Ediciones Díaz de Santos, S.A.

Iriarte, E. (2005). *Estado situacional y perspectiva del derecho informático en América Latina y el Caribe*. CEPAL. Naciones Unidas. Consultado el 28 de agosto de 2008 en
http://www.cepal.org/publicaciones/DesarrolloProductivo/5/LCW25/LCW25.pdf

Palazzi, P. (2002). *La transmisión internacional de datos personales y la protección de la privacidad.* Argentina: AD-HOC S.R.L.

Sarra, A.V. (2000). *Comercio electrónico y derecho: aspectos jurídicos de los negocios en Internet.* 1. ed. Buenos Aires, Argentina : Astrea.

Reidenberg, J. (1999). *Privacidad y comercio electrónico en los Estados Unidos.* Consultado el 20 de febrero de 2009 en http://reidenberg.home.sprynet.com/Privacidad-USA.htm

Téllez, J. (2004).*Derecho Informático*. 3 ed. México: McGraw Hill/Interamericana Editores S.A.

Vega, J. (2005). *Contratos electrónicos y protección de los consumidores*. Madrid: Reus S.A.

Materiales normativos consultados

Constitución Política de Chile. (2005). Chile. Consultado el 18 de octubre de 2008 en http://www.bcn.cl/pags/legislacion/leyes/constitucion_politica.htm

Constitución Política de la República de Colombia de 1991 con reformas hasta el 2005. (2005). Consultado el 18 de octubre de 2008 en
http://pdba.georgetown.edu/Constitutions/Colombia/col91.html

Constitución Política de Costa Rica (2002). Consultado el 18 de octubre de 2008 en http://www.constitution.org/cons/costa_rica/costa_rica.htm

Constitución Política de Ecuador. (1998). Consultado el 18 de octubre de 2008 en http://www.presidencia.gov.ec/modulos.asp?id=109

Constitución Política de los Estados Unidos Mexicanos. (2002). Consultado el 18 de octubre de 2008 en
http://constitucion.presidencia.gob.mx/index.php?idseccion=216

Constitución Política del Perú.(2000). Consultado el 18 de octubre de 2008 en
http://www.tc.gob.pe/legconperu/constitucion.html

*Convención Americana sobre Derechos Humanos "Pacto de San José". Del 7 al 22 de noviembre de 1969. Consultado el 5 de febrero de 2009. www.iij.**derecho**.ucr.ac.cr/.../LEYES%20Y%20**CONVENIO**S%20INTERNACIONALES/*

Decreto Legislativo 295 Código Civil. Publicado 25.07.84. Perú. Consultado el 8 de setiembre de 2008 en http://www.cajpe.org.pe/rij/bases/legisla/peru/codciv.htm

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. DO L 281 de 23 de noviembre de 1995. Consultado el 5 de setiembre de 2008 en:http://europa.eu.int/spain/novedades/documentos/31995L46.htm

Decisión 2000/520/CE de la Comisión de 26 de Julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. Consultado el 3 de mayo de 2009 en

https://www.agpd.es/upload%2FCanal_Documentacion%2Flegislacion%2FUnion%20Europea%2FDecisiones%2FB.12%29%20Decisi%F3n%20%20sobre%20la%20adecuaci%F3n%20conferida%20por%20los%20principios%20de%20puerto%20seguro.pdf

Decisión 2002/16/CE de la Comisión Europea Publicada el 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE. Consultado el 28 de marzo de 2009 en:http://www.cpsr-peru.org/bdatos/decisiones/europa/Decision2002_16_CE_clausulastipotercerospaises.pdf/view

Directiva 2002/CE relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la directiva 95/46/CE. Decisión de la Comisión del 27 de diciembre del 2001. Consultado el 17 de octubre de 2008 en: http://www.cpsr-peru.org/bdatos/decisiones/europa/Decision2002_16_CE_clausulastipotercerospaises.pdf

Proyecto de documento de trabajo sobre el funcionamiento del acuerdo de puerto seguro. Grupo de trabajo sobre protección de datos art. 29. 11194/02/ES WP 62. 2 de julio 2002. Consultado el 26 de octubre de 2008 en:http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp62_es.pdf

Ley Orgánica 15/99 de protección de datos de carácter personal (LOPD). 13 diciembre 1999. B.O.E. 14-12.99. España. Consultado el 26 de marzo de 2009 en http://protecciondedatos.urjc.es/PD/legislacion/index.php

Ley 34/2002 sobre telecomunicaciones y servicios de la sociedad de la información y del comercio electrónico, de 11 de julio. España. Consultado el 11 de setiembre de 2008 en http://209.85.165.104/search?q=cache:f9TFWX0B2-YJ:travesia.mcu.es/documentos/ley_34_comercio_elec.pdf+Ley+34/2002&hl

=es&ct=clnk&cd=4&gl=cr

Ley19.628 Sobre Protección de la Vida Privada o Protección de Datos de Carácter Personal. Publicada en el Diario Oficial de 28 de agosto de 1999. Chile. Consultado el 21 de marzo de 2009 en http://www.informatica-juridica.com/anexos/anexo137.asp

Ley 67 de Comercio Electrónico, Firmas y Mensajes de Datos.17 de abril de 2002. Ecuador. Consultado el 21 marzo 2009. http://www.corpece.org.ec/

*Ley 7472 Promoción de la Competencia y Defensa Efectiva del Consumidor***.** Asamblea Legislativa. Costa Rica. 1995. Consultado 23 de diciembre de 2008 en http://www.asamblea.go.cr/ley/leyes_nombre.htm

*Ley Federal de Protección al Consumidor***.** Publicada en el Diario Oficial de la Federación el 24-12-1992. México. Consultado el 20 de octubre de 2008 en: http://www.economia.gob.mx/pics/p/p1376/L34.pdf

Proyecto de ley estatutaria 143-2003 por la cual se dictan disposiciones para la protección de datos de carácter personal y se regula la actividad de recolección, tratamiento y circulación de los mismos. Colombia. **Consultado el 10 de noviembre de 2008 en** http://www.cpsr-peru.org/privacidad/privfinanciera/habeasdata_defpueblo.pdf

Proyecto de ley estatutaria 071 de 2005 Cámara por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera y crediticia, y se dictan otras disposiciones. 10 de agosto de 2005. Ministerio de Hacienda. Colombia. Consultado el 11 de noviembre de 2008 en:h ttp://www.cpsr-peru.org/privacidad/privfinanciera/proy071-2005camara.pdf

Proyecto de ley 15178 de Protección de la persona frente al tratamiento de datos personales. Asamblea Legislativa. Costa Rica. 2003. **Consultado el 4 de febrero de 2009 en** http://www.asamblea.go.cr/proyecto/15100/15178.doc.

Proyecto 14.785 que adiciona un nuevo capítulo denominado Del Recurso de Hábeas Data al Titulo III de la Ley 7135 de 11 octubre de 1989. 18 junio de 2002. Asamblea Legislativa. Costa Rica. Consultado el 5 de febrero de 2009. http://asamblea.racsa.co.cr/proyecto/exp_14785.htm

Proyecto de ley 14029 Derecho de acceso a Internet. Asamblea Legislativa. Costa Rica. 2001. Consultado el 4 de febrero de 2009 en: http://www.asamblea.go.cr/proyecto/14000/14029.doc

Ley 8131 de Administración Financiera de la República y Presupuestos Públicos. Asamblea Legislativa. Costa Rica. 2001. Consultado el 4 en febrero 2009. http://asamblea.racsa.co.cr/ley/leyes_a1.htm

Ley 4573. Código Penal, *con reformas de la Ley 7899 del 3 de agosto de 1999*. Asamblea Legislativa. Costa Rica. 1970. Consultado el 20 enero de 2009 en http://www.secmca.org/archivos/Codigo%20Penal.pdf.

(1995). *Ley No.7557. Ley General de Aduanas*. Asamblea Legislativa. Costa Rica. Consultado el 3 de abril de 2009 en: http://www.racsa.co.cr/asamblea/ley/leyes/7000/7557.doc

(1971). *Ley 4755 Código de Normas y Procedimientos Tributarios.* Asamblea Legislativa. Costa Rica. Consultado el 1 de febrero de 2009 en http://www.racsa.co.cr/asamblea/ley/leyes/6000/4755.doc

*Proyecto de Decreto que expide la Ley Federal de Protección de Datos Personales***.** Dip. Miguel Barbosa Huerta (PRD). Publicación en Gaceta Parlamentaria, 7 de Septiembre de 2001. Secretaría de Servicios Parlamentarios. México. **Consultado el 5 de febrero de 2009 en** http://www.cddhcu.gob.mx/servicios/datorele/cmprtvs/1po2/set/2.htm

Proyecto de Ley de Protección de Datos. R.M. No.94-2002-JUS. Diario Oficial El Peruano 23 de julio de 2004. Perú. **Consultado el 11 de noviembre de 2008 en**: https://www.agpd.es/upload/Canal_Documentacion/legislacion/ProyectoProteccionDatosPers-peruano.pdf