DERECHO DE PROTECCIÓN DE LOS DATOS EN EL MARCO DEL COMERCIO ELECTRÓNICO: PRINCIPIOS DE RESPONSABILIDAD

*Gladys S. Rodríguez**

Abstract: Data Protection Law under the Framework of Electronic Commerce: Responsibility Principles
Though numerous Latin-American countries have given constitutional recognition to the protection of personal data, few data protection laws have been enacted until the present. Nevertheless, the development of information society's services, especially the acquisition of goods and the provision of services across the internet, favors the treatment and indiscriminate interchange of data. This allows that the different companies that offer their services in the net should store important data related to personal aspects of users in their respective data bases. For those reasons, this paper intends to explain the scope of data protection law, especially in the context of the final consumer. It will further analyze which alternate and legal mechanisms of data protection can be implemented in the internet, and which is the national and international treatment as for privacy and intimacy that is given to technological elements, like the e-mail. Finally, it will expose the existing discrepancy in the area of extra contractual informatics' liability. This research is based upon a documental and legislative review, as well as an iusphilosophical analysis of the topic. It is concluded that Latin America will have to do efforts in order to achieve a harmonization of the laws on this matter.

Key Words: Data Protection, Data Bases, Extra contractual informatics' liability.

SUMARIO:

* Universidad del Zulia, Facultad de Ciencias Jurídicas y Políticas, Instituto de Filosofía del Derecho, Sección de Investigación Informática Jurídica y Derecho Informático, Maracaibo, Estado Zulia, Venezuela. Correo: gr1970ve@yahoo.es.

1. Introducción

En 1990 fue la época en que se produjo el crecimiento espectacular de Internet, que resultó en una propulsión tecnológica inesperada de todos los procesos donde el hombre participa. Entretanto, el contexto institucional para las relaciones económicas, sociales, políticas y jurídicas internacionales también empezó a cambiar [18] y, con este nuevo fenómeno tecnológico se inicia una nueva forma de interrelación intersubjetiva. Pero, antes de ingresar en el estudio del tema propuesto, corresponde recordar algunos antecedentes sobre el tema, en [2], [5], [7] y [10] coinciden en el estudio de *habeas data* partiendo de una comparación entre los países, especialmente latinoamericanos y de Europa, resaltando el caso de España, se han detenido a estudiar la naturaleza de esta institución en cuanto a determinarlo como derecho sustantivo y derecho adjetivo, algunos en [7] han hecho análisis además de la jurisprudencia en la materia, otros como en [2], se han enfocado en las instituciones u órganos necesarios para lograr tal protección, en [5] lo comparan con otras instituciones como el *habeas corpus* y el amparo. Sin embargo, todos coinciden en la necesidad de regular y armonizar la figura de la protección de datos. En este contexto entonces, resulta imperioso responder a la pregunta: ¿de qué manera podemos defender los derechos humanos y/o fundamentales, particularmente los datos de las personas que se ven afectados o impactados ante el desarrollo de la tecnología de información y comunicación?, es ésta la principal interrogante, aunque no la única, que nos hemos planteado durante el desarrollo de esta investigación; y es que resulta lógica tal interrogante ante la realidad del fenómeno tecnológico, pues día a día son millones los usuarios que confluyen en un espacio que no tiene límites ni fronteras, como es Internet y donde los derechos humanos fundamentales son fácilmente vulnerados.

Ahora bien, también resulta relevante aclarar algunos términos, en primer lugar, sobre el carácter de derecho humano o fundamental que implica la protección de los datos, la pregunta pertinente es si se trata de un derecho fundamental, pues está claro que se trata de un derecho humano. Ante ello, cabe igualmente preguntarnos, si existe o no diferencia; en principio debe decirse que los derechos fundamentales y su formulación jurídico-positiva como derechos constitucionales son un fenómeno relativamente reciente, aunque sus raíces filosóficas se remontan, y se hallan íntimamente ligadas, a los avances históricos del pensamiento humanista. Es así que desde la antigüedad la tesis postulada, en el seno de la doctrina estoica, sobre la unidad universal de los hombres, o la afirmación cristiana de la igualdad esencial de todos los seres humanos ante Dios, constituyó un aldabonazo para despertar y alentar la conciencia de la dignidad humana. Por su parte, al hablar de derechos humanos suelen ser caracterizados desde el positivismo a partir del fenómeno de su internacionalización. Se trata de un proceso ligado al reconocimiento de la subjetividad jurídica del individuo por el Derecho Internacional.

En efecto el elemento diferenciador de estas dos categorías es el diferente grado de concreción positiva. De allí que «derechos humanos» aparece como un concepto de contornos más amplios e imprecisos que la noción de los «derechos fundamentales». «Los derechos humanos» suelen venir entendidos como un conjunto de facultades e instituciones que, en cada momento histórico, concretan las exigencias de la dignidad, la libertad y la igualdad humanas, las cuales deben ser reconocidas positivamente por los ordenamientos jurídicos a nivel nacional e internacional. En tanto, con la noción de los «derechos fundamentales» se tiende a aludir a aquellos derechos humanos garantizados por el ordenamiento jurídico positivo, en la mayor parte en los casos en su normativa constitucional, y que suelen gozar de una tutela reforzada... [9], como es a través de Acuerdos Internacionales o Tratados.

La anterior disertación encuentra sentido pues, al hablar de la protección de los datos personales, necesariamente acudimos a su género más próximo, los derechos humanos, pero ha sido tal el impacto que las nuevas tecnologías, especialmente la informática, han producido en el hombre-ciudadano, que la mayoría de las Constituciones han incorporado esta tutela hacia los datos y, en algunos casos, abarcan lo referente a la privacidad e intimidad o lo contemplan como otro derecho fundamental, caso de la Constitución nacional venezolana, lo cual hace un reconocimiento de tales derechos como derechos fundamentales, por lo que aspiramos que en nuestro país se logre dictar una legislación apropiada para el desarrollo e implementación de la figura de *habeas data*, así como el de la armonización de normas a nivel internacional y particularmente regional.

Por otra parte debemos entender por datos de acuerdo en [19] como el antecedente necesario para llegar al conocimiento exacto de una cosa o para deducir las consecuencias legítimas de un hecho. En tanto comercio electrónico debe ser entendido como aquellas actividades que se desarrollan antes, durante y luego del acto de comercio, que implica transferencia de bienes o servicios a través de medios electrónicos. Y, finalmente, *habeas data* se señala en [5] como una garantía procesal constitucional, configurativa de un amparo especializado, con finalidades específicas.

Por ello, el presente trabajo establecerá el alcance del derecho de protección de datos, especialmente en el contexto del consumidor final; indicará cuáles mecanismos alternos y legales de protección de los datos pueden ser implementados en Internet; describirá cuál es el tratamiento nacional e internacional en materia de privacidad e intimidad que se le dan a elementos tecnológicos, como el *e-mail*, y, finalmente, exponer la discrepancia existente en el ámbito de la responsabilidad extracontractual informática.

2. Tratamiento del derecho de protección de datos: diferentes escenarios

El Derecho Constitucional incluye dentro de su objeto, no sólo las regulaciones sustanciales en relación a la organización del poder público y la consagración de los derechos, sino también desde su origen y cada vez con mayor énfasis, las previsiones adjetivas tendientes a garantizar la vigencia efectiva del ordenamiento constitucional. El ejercicio del derecho a la vigencia de la Constitución y en relación a los derechos constitucionales mediante acciones expeditas y especializadas, tiene su origen en Latinoamérica en la institución del amparo constitucional, la cual surgió a nivel constitucional en México, en la Constitución Federal de 1857. Dicha acción surgió con la finalidad de revisar la constitucionalidad de las leyes en los casos concretos que afecten derechos constitucionales, originalmente sólo individuales.[1]

En la actualidad, bajo el nombre de «amparo», en la mayoría de los casos, incluso a nivel constitucional, al menos trece ordenamientos latinoamericanos han adoptado expresamente este instituto para la protección de los derechos de la persona: Argentina (artículo 43 de la Constitución); Bolivia (artículo 19 de la Constitución); Costa Rica (artículo 48 de la Constitución); El Salvador (artículo 182, ord. 1° de la Constitución); Guatemala (artículo 265 de la Constitución); Honduras (artículo 183 de la Constitución); México (artículo 107 de la Constitución); Nicaragua (artículo 188 de la Constitución); Panamá (artículo 50 de la Constitución); Paraguay (artículo 134 de la Constitución); Perú (artículo 200 de la Constitución); Uruguay (artículos 7 y 12 de la Constitución) y Venezuela (artículo 49 de la Constitución). Sin embargo, en el caso que nos ocupa, esta protección de los datos de las personas está contemplada, en el caso particular de Venezuela, en el artículo 28 de la Constitución vigente, en forma distinta a la figura de amparo, es decir, es protegido a través de una institución muy *sui generis* que la doctrina ha denominado *habeas data*.

Bajo este contexto protector, al revisar la labor por parte de los Estados americanos, en ejercicio de su soberanía, se puede observar que se han adoptado una serie de instrumentos internacionales que se han convertido en la base de un sistema regional de promoción y protección de los derechos humanos. Dicho sistema normativo reconoce y define estos derechos, establece obligaciones tendientes a su promoción y protección, y crea órganos destinados a velar por su observancia. Este sistema interamericano de protección de derechos fundamentales se inició formalmente con la aprobación de la Declaración Americana de los Derechos y Deberes del Hombre en la Novena Conferencia Internacional Americana celebrada en Bogotá en 1948, en el marco de la cual se adoptó la Carta de la OEA que proclama los derechos fundamentales de la persona humana. [18]. Asimismo, se aprobaron varias resoluciones en torno a los Derechos Humanos, pero a los fines del presente trabajo, vale destacar que, durante su 69.° período ordinario de sesiones (Río de Janeiro, agosto 2006), el Comité Jurídico Interamericano consideró el documento *Cuestionario para los Estados miembros de la OEA respecto a la legislación sobre el acceso a la información y la protección de datos personales, especialmente en forma electrónica.*

El propósito del referido Cuestionario es la posible elaboración de un instrumento jurídico interamericano sobre estos dos temas, y aprobó un cuestionario que fue remitido a los Estados miembros a través de la Secretaría General, invitándolos a contribuir así al estudio del Comité Jurídico en la materia; no obstante, sólo se han recibido tres respuestas, por

lo cual, para el 70.° período ordinario de sesiones (San Salvador febrero-marzo 2007), se resolvió entre los aspectos más importantes, los siguientes:

- 3. Solicitar a la Secretaría General que remita al Consejo Permanente el informe actualizado *Derecho de la Información: acceso y protección de la información y datos personales en formato electrónico* (CJI/doc.25/00 rev.2, de 7 de febrero de 2007) solicitado por la Asamblea General en su antes citada resolución.
- 5. Solicitar a los Estados miembros que todavía no lo hayan hecho responder al cuestionario antes mencionado.
- 6. Mantener el tema del Derecho de la información en su agenda y solicitar al relator que presente un informe actualizado en su próximo período ordinario de sesiones, tomando en cuenta las respuestas adicionales que se puedan recibir por parte de los Estados miembros.[15]

La tarea de protección de los Derechos Humanos, se extiende y adquiere un nivel universal cuando las Naciones Unidas se han ocupado del tema de los Derechos Humanos y, es así que desde el 10 de diciembre de 1948, la Asamblea General de las Naciones Unidas aprobó y proclamó la Declaración Universal de Derechos Humanos. Tras este acto histórico, la Asamblea pidió a todos los Países miembros que publicaran el texto de la Declaración y dispusieran que fuera distribuido, expuesto, leído y comentado en las escuelas y otros establecimientos de enseñanza, sin distinción fundada en la condición política de los países o de los territorios. De esta manera, en sus disposiciones vale destacar el artículo 12 de la referida Declaración que expone:

> Nadie será objeto de injerencias arbitrarias en su vida privada, [...] o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley [...].

Sobre el tema de la protección de los datos bajo un sistema informático, las Naciones Unidas han elaborado unas *Directrices para la regulación de los archivos de datos personales informatizados*. Tales Directrices fueron adoptadas mediante Resolución n.° 45/95 de la Asamblea General de 14 de diciembre de 1990; por supuesto, los procedimientos para llevar a la práctica las normas relativas a los archivos de datos personales informatizados se dejan a la iniciativa de cada Estado.

En definitiva, no existe sólo una preocupación por parte de cada uno de los Estados, hacia su interior, por velar por la protección de los datos ante el auge de las Tecnologías de Información y Comunicación (TICs) a través de la consagración de tal derecho fundamental en sus Constituciones y/o leyes, sino a nivel internacional, los organismos internacionales también hacen su esfuerzo.

Todos estos esfuerzos legislativos al interior de los países e internacionalmente es motivado al desarrollo indiscutible de los servicios de la sociedad de la información, en especial, ante el incremento de la adquisición de bienes y prestaciones de servicios a través de Internet, lo cual favorece el intercambio indiscriminado de datos. Esta situación permite que las empresas cuando ofrecen sus servicios en la red, almacenen información importante relacionada con aspectos personales de los usuarios en sus respectivas bases de datos, creándose una inquietud por la protección de dichos datos.

Cuando se realiza una compra en Internet, y por ello, nos interesa la situación del consumidor final, aquél que adquiere bienes y servicios para su consumo o uso particular o familiar, sin fines de lucro o ganancia alguna; generalmente, se llena un formulario de pedido del cual se refleja información no sólo sobre los bienes que se adquieren, sino también sobre el comportamiento ante determinados productos o servicios, dejando huellas, entre otras circunstancias, de las preferencias en los sistemas de ventas, formas de pago, y otros datos de carácter personal, como el domicilio, sexo, edad, profesión y número de cuentas bancarias, información que permite la creación de perfiles y estándares automatizados, mediante la categorización de sujetos gracias al tratamiento de esos datos, que luego son tratados con fines comerciales de publicidad y mercadeo, causando graves perjuicios en la esfera íntima del individuo. [11]

Además, no sólo es posible dejar huellas haciendo una operación comercial por la red, simplemente al revisar los distintos sitios web, ya se está dejando datos que son captados por el sistema informático, tal como sucede con los denominados *cookies*, o pequeños ficheros de datos generados en el computador del usuario en forma de archivos de texto, gracias a instrucciones que los servidores web envían a los programas de los computadores. Esto permite el acceso a información del usuario sobre sus datos personales o sobre cualquier otra circunstancia, ya que pueden ser leídos desde el exterior gracias al interfaz con el servidor, permitiendo hacer perfi-

les de los usuarios, en la mayoría los casos, sin su consentimiento y conocimiento, por lo cual, no es el tratamiento de los datos personales en sí lo prohibido, sino el tratamiento ilegal de esos datos.

2.1. Ambivalencia de la protección de datos en el comercio electrónico

La idea es ofrecer protección a los datos como algo que puede ayudar a mejorar las expectativas de éxito del negocio electrónico, y que al mismo tiempo, constituya un elemento indispensable para que podamos vivir en la sociedad de la información, sin que las TICs afecten negativamente nuestra dignidad como personas. Para ello, se debe conocer sucintamente cómo es la estructura de protección de los datos en Venezuela y algunos países latinoamericanos.

Nos guste o no (que sí nos gusta), pertenecemos a una cultura que considera que la dignidad humana es superior a otros valores, también importantes, pero de rango inferior, como la eficiencia económica y la eficacia administrativa.

En Latinoamérica y en Venezuela, para evitar que la imparable informatización de la sociedad afecte a nuestra dignidad, el derecho a la protección de datos se ha construido como un derecho fundamental de la persona. Esto es lo que dice el artículo 28 de la Constitución Nacional Venezolana:

> Toda persona tiene derecho de acceder [...] a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados.... conocer el uso y su finalidad,... solicitar [...] la actualización, la rectificación o la destrucción de aquéllos [...].

Desde luego, **que un derecho sea considerado fundamental no quiere decir que sea un derecho absoluto** (no es el caso), pero tiene consecuencias muy importantes. Por ejemplo, cualquier ley sobre la materia debe respetar lo que los juristas llamamos el contenido esencial del derecho; y, en caso de que surjan dudas en la interpretación de las normas que regulan la materia, se debe optar siempre por la interpretación menos restrictiva.

En mayor o menor grado, **el derecho de protección de datos afecta a todos los ámbitos de la vida en que se manipule información personal**, o sea, a prácticamente todos. Tiene, pues, un enfoque inclusivo (porque el concepto de dato personal comprende cualquier información concerniente a la persona) y dinámico, porque regula cualquier operación de tratamiento de datos personales (recopilación, utilización, transmisión, revelación, conservación, cancelación, etc.).

Sin embargo, en Venezuela aún no se ha promulgado una ley en la materia. Existe un Anteproyecto de Protección de Datos y *Habeas Data* para Venezuela que todavía se encuentra en discusión desde el año 2004. Está vigente, sin embargo, la Ley sobre Protección a la Privacidad de las Comunicaciones de fecha 16 de diciembre de 1999.

Por su parte, Argentina tiene consagrada en su Constitución la figura de *habeas data* y posee una Ley n.° 25.326, Ley sobre Protección de los Datos Personales del año 2000.

Perú también consagra en su Constitución la figura de protección y posee una Propuesta de Legislación de Protección de Datos del Ministerio de Justicia del Perú.

En su caso, Colombia tiene consagrado el derecho en su Constitución pero recién aprobó el 29 de mayo la Ley de *Habeas Data*.

En Chile se discute el Proyecto de Ley sobre *Habeas Data*.

En Bolivia se dictó en el año 2004 el Decreto n.° 27329, Decreto de Transparencia y Acceso a la Información Gubernamental.

Por su parte, Brasil, en el año 1997, promulgó el Decreto n.° 27329 27329, Decreto de Transparencia y Acceso a la Información Gubernamental.

México posee desde el año 2004 el Proyecto Ley Federal de Protección de Datos Personales.

Paraguay tiene una Ley de Información de Carácter Privado y Uruguay tiene desde el 2004 una Ley de *Habeas Data* n.° 17.838.

Es evidente que existe una materialidad legislativa en la materia de *habeas data*, pero no obstante, diariamente ese consumidor final, cuando accede a la red, se ve indefenso ante la imposibilidad de controlar o autodeterminar la información que sobre él y sus bienes existen.

Por ello, resulta necesario indicar algunos mecanismos legales y técnicos para proteger la data.

3. Mecanismos alternos y legales de protección

Más del 90% de los datos provienen directamente del propio interesa-

do, y casi siempre se cuenta con su consentimiento. **Lo que importa, entonces, es que ese consentimiento se forme válidamente.**

Para ello, las leyes en la materia deberán determinar una serie de condiciones para la prestación válida del consentimiento, recordando que el consentimiento se entiende como **manifestación de voluntad libre, inequívoca, específica e informada.**

El requisito ‹informada› da lugar al llamado derecho de información en la recogida de los datos que consagran las distintas Constituciones.

El derecho de información tiene especial importancia porque condiciona la validez del consentimiento (que debe ser informado), establece los límites al tratamiento (finalidad, necesidad) y permite el ejercicio de los derechos del interesado. Para que el consentimiento sea válido se requiere que los datos no se recaben por medios fraudulentos, desleales o ilícitos (principio de lealtad). **Quien consienta en que sus datos sean tratados debe saber qué y para qué consiente.** Todo consentimiento debe basarse en la información, si bien, en cuanto a ésta, la ley diferencia entre los siguientes supuestos:

Si los datos son recabados del propio interesado, debe proporcionarse información previa e inequívoca sobre: (1) la existencia y la finalidad del fichero de datos, así como de posibles cesiones de datos a terceros; (2) si las respuestas (los datos) son obligatorias u optativas; (3) las consecuencias de que el interesado no proporcione los datos; (4) la posibilidad de ejercitar ciertos derechos; (5) la identidad y dirección del responsable del fichero. Se permite excluir la información (2), (3) y (4), si ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

La Red Iberoamericana de Protección de Datos ha desarrollado un documento sobre las Directrices para la armonización de datos en la Comunidad Iberoamericana, del cual se puede evidenciar lo siguiente:

Se han presentado algunos principios, a saber:

- Los datos deberán ser tratados de modo leal.
- Los datos deberán ser tratados para fines concretos.
- El tratamiento deberá efectuarse sobre la base del consentimiento del interesado o como consecuencia de algún otro fundamento legítimo y previsto legalmente.
- Toda persona tendrá los derechos de acceso, rectificación y cancelación al tratamiento.
- Deberá existir una autoridad independiente encargada de velar por la garantía del derecho.

Por otra parte, distintos instrumentos internacionales, procedentes de Organismos Supranacionales de los que son miembros todos o parte de los Estados Iberoamericanos, han venido a establecer los principios básicos que configuran el derecho a la protección de datos personales.

Así, la Organización de Cooperación y Desarrollo Económico (OCDE) delimita estos principios, enumerando como básicos los siguientes.

1. Aplicación a todo tratamiento de datos del sector público y del privado.
2. Interpretación restrictiva de las posibles exclusiones a la aplicación de los principios.
3. Principio de limitación de la recogida.
4. Principio de calidad de los datos.
5. Principio de especificación de la finalidad.
6. Principio de limitación de uso.
7. Principio de salvaguardas de seguridad.
8. Principio de apertura.
9. Principio de participación individual (*Habeas Data*).
10. Principio de responsabilidad.
11. Garantías de la circulación transfronteriza, ininterrumpida y segura, de los datos personales, entre los Estados que observen los principios.
12. Establecimiento de sanciones y recursos suficientes en caso de incumplimiento.

A su vez, deben tenerse en cuenta las Directrices para la regulación de los archivos de datos personales informatizados, adoptadas mediante Resolución n.° 45/95 de la Asamblea General de las Naciones Unidas, de 14 de diciembre de 1990, a los cuales nos referimos en párrafos anteriores, que consideran como garantías mínimas que deben prever las legislaciones nacionales los siguientes principios:

1. Principio de legalidad y lealtad.
2. Principio de exactitud.
3. Principio de especificación de la finalidad.
4. Principio de acceso de la persona interesada.
5. Principio de no discriminación.
6. Limitación de la facultad para hacer excepciones.

7. Principio de seguridad.
8. Supervisión y sanciones, a través de una autoridad que deberá ofrecer garantías de imparcialidad, independencia y competencia técnica.
9. Flujo transfronterizo de datos basado en la similitud de las salvaguardas.
10. Campo mínimo de aplicación general a todos los archivos informatizados públicos y privados.

En el marco regulatorio, otro aspecto a considerar es el de la autorregulación, la cual constituye una alternativa menos rígida, especialmente, frente a la actividad de comercio electrónico, pues no es un secreto que las normas de protección de datos constituyen para el comercio una imposición externa que incrementa los costos de las transacciones de las empresas y constituye, por tanto, una barrera no tarifaria para su desarrollo. Recuérdese que las normas cuando son vistas como una injerencia en el sistema, éste tiende a no cumplirlas, aun frente a la amenaza de correlativas sanciones. Por ello, resulta beneficioso el clima de colaboración de los distintos actores que participan en el sector, siendo la alternativa la Autorregulación.

Existen dos formas elementales de concebir la autorregulación social. En un sentido débil o impropio, cualquier tipo de regla privada constituye un mecanismo de autorregulación. Ésta es, por así decir, la visión estadounidense del término, su principal inconveniente es que tarde o temprano prevalecen las posiciones económicas y de poder, sin que medie ningún control jurídico. En cambio, en un sentido fuerte o propio, la autorregulación denota el control jurídico de la autorregulación social, esto es, el diseño de un marco de derecho cogente dentro del cual los agentes sociales involucrados puedan dotarse de sus propias normas específicas. Sólo así tendrá sentido establecer un régimen de autorregulación a fin de articular un cierto consenso social [14].

Cuando se trata del comercio electrónico, esta posibilidad es muy ventajosa desde el punto de vista de la protección de datos, pues se logra un nivel de protección más amplio, se subsanan algunos vacíos legislativos y se toma los mecanismos de composición y resolución alternativa de conflictos que incluyen estos programas de autorregulación, imprescindibles para los múltiples conflictos o litigios propios del sistema general de protección de datos, descongestionándose los órganos jurisdiccionales.

Otro mecanismo es el Acuerdo entre las naciones. En este sentido se han nombrado algunos a nivel europeo, a nivel de las Naciones Unidas de la OCDE, y ante ello surge la inquietud, pues es un hecho relativamente sumido que la protección de datos personales en Internet no puede lograrse sin protección de datos en (y desde) los Estados Unidos de América. Porque Internet es una red interconectada de empresas, en su mayoría, norteamericanas; por ello, se presentan contradicciones o ambivalencias entre el derecho fundamental a la protección de datos reconocido por la mayoría de las legislaciones y las reglas del mercado y la cultura jurídica de los Estados Unidos de América.

Sin embargo, es frente a esta contradicción donde pueden surgir instituciones híbridas capaces de funcionar en una sociedad global del conocimiento.

En materia de protección de datos, éste es el papel que juega el Acuerdo de *Safe Harbor*. Este Acuerdo resuelve la incompatibilidad entre un sistema de disciplina legislativa y estatal de la protección de datos y otro sistema basado en la autorregulación débil en casi todos los sectores de su economía. El nuevo sistema, además, trasladaría a la cultura jurídica estadounidense, de una forma no traumática, el modelo fuerte de autorregulación, equilibrando así la concepción *iusfundamental* que el derecho de protección de datos tiene frente a la concepción meramente comercial de los datos personales como información, y de esta manera los Estados beneficiarse de ese flujo informativo.

Las instituciones híbridas son esfuerzo para crear interfaces entre diferentes sistemas jurídicos que están siendo interconectados crecientemente por efecto de la globalización, se busca un mínimo que es la coordinación y armonización.

Después de haber revisado los mecanismos legales como opciones para la protección de datos, queda por evidenciar algunos de carácter técnico, que complementarían tal protección, a saber:

Vale decir, que las soluciones técnicas de protección de datos se agrupan bajo el epígrafe de tecnologías favorecedoras de la privacidad (*Privacy Enhancing Technologies: PETs)*. La categoría es muy heterogénea, abarca desde los anuladores de *cookies*, hasta los repetidores de correo (*remailers)* y los anonimizadores de navegación, pasando por los servidores

proxy, los agentes de *software* y las aplicaciones criptográficas como PGP.

Hasta ahora las posibilidades u opciones técnicas son básicamente las siguientes según en [14]:

3.1. Plataforma de preferencias de privacidad

Esta plataforma permite a los sitios web expresar sus prácticas de privacidad en un formato estándar de modo que puedan ser leídas e interpretadas automáticamente por un agente de *software* que utiliza el usuario, en ocasiones estas políticas son apreciadas por el usuario o *cibernauta* cuando accede a algún lugar en la red.

Por ello, en sentido amplio, puede decirse que la Plataforma de Preferencia de Privacidad forma parte del código de Internet. Al integrarse directamente en el código, esta solución parece óptima en punto a reconciliar los intereses contrapuestos de la protección de datos y el comercio electrónico. Por supuesto, existen debilidades de este mecanismo, tales como no proteger al usuario de Internet en los países que carecen de ese marco legislativo; no proporciona ninguna forma de asegurar que las compañías que la utilizan sigan sus propias políticas de privacidad, ni que el sitio web que visitamos esté haciendo lo que afirma hacer, además prevalece beneficiar al propietario del sitio o del servidor web.

3.2. Agentes de software con protecciones de privacidad

Son agentes de *software* que incorporan reglas de protección de la privacidad (*Privacy Incorporated Software Agent: PISA)*, capaces de eliminar o minimizar la obtención y uso de información personal. Respecto de la plataforma de preferencias de privacidad, la ventaja que muestra este tipo de agentes es que aspiran a implementar en sus especificaciones técnicas un modelo fuerte de legislación de protección de datos. Se recomienda, por ejemplo, aplicar algún tipo de *checklist* de criterios de cumplimiento de las legislaciones existentes para que los agentes sean construidos integrando tecnologías de protección de la privacidad, e incluso que se establezca un marco de certificación de privacidad para el diseño y fabricación de los agentes.

También poseen sus limitaciones, pues ante la realidad del comercio electrónico, para el momento, no se permiten estos agentes en algunos sitios web, que los consideran incómodos o perjudiciales para el negocio, de modo que no se mantiene la funcionalidad del sistema.

3.3. El modelo de mercado: los infomediarios

Se trata de gestores o intermediarios que ayudan a los consumidores a maximizar el valor de sus datos personales. La función del *infomediario* es representar al consumidor y optimizar el valor que éste recibe a cambio de sus datos. Agregando la información y utilizando el poder de mercado que le dan los muchos clientes de su club virtual de compras, los infomediarios aspiran a crear una serie de mercado inverso, a través del cual los consumidores recuperen parte del poder de negociación.

Pese a que su funcionamiento y caracteres pueden variar según los casos, en general, el infomediario protege los datos del usuario frente a los abusos y cesiones no consentidas, proporcionándole herramientas de privacidad que tratan de asegurar un determinado nivel de anonimato (*e-mail, anónimo, filtros de spam o anuladores de cookies*).

Asimismo, el proveedor del infomediario genera y pone a disposición del consumidor perfiles sobre los vendedores, que incluyen sus ratios de venta, el volumen de devoluciones y reclamaciones, así como el grado de satisfacción de los clientes. Al mismo tiempo, el infomediario recoge y trata información completa del usuario y elabora un perfil informativo extraordinariamente profundo que cubre preferencias y transacciones de consumidor, tanto dentro como fuera de la red.

Pero, la utilización de infomediarios no está exenta de riesgos, dado que la relación entre el usuario y el infomediario se basa exclusivamente en la confianza, es preciso que existan recursos legales efectivos para el caso de que el segundo no cumpla lo que promete.

4. Concepto y principios del habeas data

Lo anterior conlleva al establecimiento de una institución jurídica que es conocida como *habeas data*, se trata de un derecho que asiste a toda persona, identificada o identificable, a solicitar la exhibición de los registros, públicos o privados, en los cuales están incluidos sus datos personales, o datos sobre sus bienes para tomar conocimiento de su exactitud; a requerir

la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación, tal cual como lo recoge el artículo 28 de la Constitución Nacional.

Etimológicamente viene del latín y significa que el sujeto a que los datos refieren pueda tenerlos, acceder a los mismos.

En [16] el *habeas data* importa una pieza del Derecho Procesal Constitucional configurativa de un amparo especializado, con finalidades específicas.

El *habeas data* es una garantía constitucional, con objetivos muy precisos, que busca que el accionante sepa:

1. Por qué motivos legales, el poseedor de la información llegó a ser tenedor de la misma.
2. Desde cuándo tiene la información.
3. Qué uso ha dado a esa información y qué hará con ella en el futuro.
4. Conocer a qué personas naturales o jurídicas, el poseedor de la información le hizo llegar dicha información. Por qué motivo, con qué propósito y la fecha en la que circuló la información.
5. Qué tecnología usa para almacenar la información.
6. Qué seguridades ofrece el tenedor de la información para precautelar que la misma no sea usada indebidamente.
7. Qué información se tiene respecto a determinada persona y para qué se almacena.
8. Si la información es actualizada y correcta y, de no serlo, solicitar y obtener la actualización o rectificación de la misma.
9. Conociendo los datos, se suprimen si no corresponde el almacenamiento, por la finalidad del registro o por el tipo de información de que se trata.

Su finalidad, entonces, consiste en proteger al individuo contra la invasión de su intimidad, ampliamente, su privacidad y honor, a conocer, rectificar, suprimir y prohibir la divulgación de determinados datos, especialmente los sensibles, evitando, pues, calificaciones discriminatorias o erróneas que puedan perjudicarlo.

La garantía de tercera generación es una garantía específica que no excluye la existencia necesaria de determinadas bases de datos que contengan determinada información.

Por ello, debe entenderse, sin perjuicio de que determinadas informaciones que no refieran a datos sensibles, pueden ser declaradas secretas por ley en razón del interés general, por ejemplo, en sede de Defensa Nacional. Esta circunstancia debe reglarse con sumo cuidado teniendo presente que es la excepción, no la regla o principio.

De lo expuesto podemos extraer los principios más importantes que la legislación comparada, con mayor o menor detalle y precisión, regula.

Entre ellos, y en primer lugar, debemos mencionar el principio de limitación de la recolección de datos, por ejemplo, datos sensibles.

La limitación también se refiere al plazo durante el cual los datos pueden estar almacenados. Es decir que, por ejemplo, en el supuesto de bases de datos de información crediticia, los datos deben suprimirse producida la prescripción de los mismos. Este principio se relaciona, íntimamente, con el que se estudia a continuación porque, en el supuesto de la limitación temporal de conservación del dato importa, sin lugar a dudas, la finalidad de la recolección.

Otro principio fundamental es el que limita la recolección a la finalidad de creación del registro. Aquí nos preguntamos, ¿para qué fue creada la base?

Si el registro efectúa almacenamiento para el cual no fue creado, en general, y para todas las personas o, específicamente, en un caso concreto, registra información de un individuo que no responde a su objeto, debe ser eliminada.

Este principio puede concluirse, aun sin reconocimiento expreso o ley que regule el *habeas data*, de los estatutos de la persona jurídica de que se trate, en el supuesto de registros administrados por personas no físicas.

También debe mencionarse el principio de seguridad. Este principio puede entenderse como seguridad en el almacenamiento a los efectos de que no se pueda ingresar ilegítimamente a las bases o, de efectuarse cesión de datos, se haga con determinados requisitos, incluido el que garantice que el cesionario cuente con la misma seguridad que el cedente.

También se lo ha entendido como el que garantiza de las posibles violaciones a la normativa que rige la materia.

Por último, existe un principio que permite al individuo con legitimación activa acceder, en sen-

tido amplio, a las bases de datos correspondientes, así como a los organismos de control, de existir.

Los principios mencionados son la columna del instituto. De los mismos deberán surgir los derechos y obligaciones fundamentales aplicables. Por otra parte, tratándose de principios generales, permitirán al intérprete observar la legislación correspondiente y, en el supuesto de vacío u oscuridad, servirán de reglas fundamentales para resolver el caso que se ventile. [13]

En el caso de Venezuela, desde el año 2004, se presentó un Anteproyecto de Ley en la materia, el cual espera por su aprobación en la Asamblea Nacional. No obstante, a nivel jurisprudencial con base en Sentencia n.° 332 de 14 de marzo de 2001 (Caso: INSACA), se han resuelto algunos aspectos para el ejercicio de este derecho, incluso se le ha dado una interpretación más amplia, si se le compara con otras naciones, como es que el ámbito de protección incluye a las personas jurídicas de cualquier naturaleza, sin embargo, nos encontramos en mora legislativa, lo cual significa un perjuicio para quienes a diario acceden a la red.

En Venezuela también se aprobó desde el año 1991 en la Gaceta Oficial n.° 34863, la Ley sobre Protección a la Privacidad de las Comunicaciones, cuyo artículo 1 establece: «La presente ley tiene por objeto proteger la privacidad confidencialidad, inviolabilidad y secreto de las comunicaciones que se produzcan entre dos o más personas».

Y, de manera conjunta, con la ley especial sobre delitos informáticos venezolana de fecha 6 de septiembre de 2001, cuyo objeto es:

> Artículo 1.- La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Por otra parte, la Ley de Protección al Consumidor y Usuario introduce en su artículo 37 una norma de especial relevancia jurídica, sobre todo para fines de comercio electrónico, al establecer la obligación de garantizar la privacidad y confidencialidad de los datos de los usuarios, imponiendo al proveedor el deber de utilizar medios adecuados que permitan la privacidad de los consumidores y usuarios, así como la confidencialidad de las transacciones realizadas, de forma tal que la información intercambiada no sea inteligible para terceros no autorizados que tengan acceso, ya sea voluntaria o accidentalmente.

En la misma disposición se establece la obligación de señalar:

> 2. [...] de manera suficiente los fines para los cuales el proveedor utilizará esta información a terceros no relacionados con el negocio, y bajo qué circunstancias pudiera darse este supuesto.

Asimismo, el artículo 38 *ejusdem* plantea que los proveedores tienen la obligación de otorgar al consumidor o usuario la posibilidad de que pueda escoger, entre la información recolectada, aquélla que no podrá ser suministrada a terceras personas; y de indicar si el suministro de información sobre éstos es parte integrante del modelo de negocio del proveedor. Con esta disposición se pretende proteger tanto los casos en los que el propio consumidor suministra sus datos como aquellos en donde la información es captada por el propio sistema informático, como sucede con los *cookies*.

Es notorio, entonces, que existen esfuerzos, pero es imprescindible una ley en la materia, pues aspectos como el tratamiento de datos de carácter personal, motivado principalmente por el intercambio y la venta de bases de datos entre las distintas empresas alojadas en Internet, es uno de los aspectos que mayor temor crea en los usuarios en el momento de suministrar su información. Otro aspecto considerado fundamental y deberá ser abordado por las diversas legislaciones, coadyuvando a la referida armonización normativa, en cuanto al momento del tratamiento internacional de datos, pues de nada vale tener una legislación protectora si, al salir de la frontera, en el resto de los países hay insuficiencia en la protección, o, lo que es peor, no se encuentra tal regulación.

5. Principios de responsabilidad

Si bien antiguamente existían unas limitaciones de carácter espacial y temporal para el acceso a la información, las modernas técnicas de comunicación y la informática superan todas estas barreras, posibilitando el conocimiento ordenado y relacionado de los datos, de forma que puede dibujarse inequívocamente el perfil de la persona, y ser utilizado posteriormente para elaborar un juicio sobre ella. Por este motivo se establecen fronte-

ras que limitan la utilización mecanizada, ordenada y discriminada de los datos sobre los individuos [3].

Una de esas fronteras son las firmas electrónicas, los certificados electrónicos en el documento que contenga el o los datos personales; crear controles de acceso; definir y documentar funciones y obligaciones de cada una de las personas con acceso a estos datos personales; copias de respaldo, al menos semanalmente; la identificación del tipo de información que contienen, ser inventariados y almacenados en lugar de acceso restringido, son fronteras que se han venido implementando, pero una frontera importante desde el ámbito legal es la responsabilidad del tenedor de la base de datos y, más cuando se está en el escenario del comercio electrónico, y por ello a ella nos dedicaremos en seguida.

Se conoce que la responsabilidad y, particularmente, a los fines del presente trabajo, la responsabilidad civil puede dividirse en: a) responsabilidad civil contractual, que se origina cuando el deudor de una obligación que emana de un contrato causa daño al acreedor; y b) responsabilidad civil extracontractual, que tiene lugar cuando una persona denominada *agente*, causa un daño a otra persona llamada *víctima*, y sin que esta acción lesiva tenga conexión o vínculo jurídico anterior, entre el *agente* y la *víctima*, o sea, independientemente de todo contrato, en consecuencia, el vínculo jurídico se genera a partir del hecho ilícito. [6]

Partiendo de lo expuesto, cabe destacar que el tenedor o propietario de la base de datos que contiene datos de carácter personal, debe comportarse como un buen padre de familia, esto significa, que debe actualizar la data, verificar las solicitudes de los titulares de esos datos, en cuanto a la rectificación o supresión de los mismos, por lo que, generalmente, si partimos del supuesto de que los ciudadanos, cuando dan sus datos, lo hacen con conocimiento.

Necesariamente, esto último implica un acuerdo o contrato para utilizar esos datos para los fines que se han obtenido o ingresado a la base de datos. Este escenario no causa mayor intranquilidad, pues existe una relación jurídica que implica deberes y derechos reconocidos y aceptados para ambas partes, y, al momento del incumplimiento, es más fácil determinar la responsabilidad contractual.

Sin embargo, el común denominador es que no damos nuestro consentimiento para el tratamiento de los datos de carácter personal. En la mayoría de las ocasiones ingresamos datos que nos solicitan sin mayor reparo o escrúpulo, y es allí donde se presenta el mayor inconveniente. Por ello los daños que pueden sufrir los individuos no unidos contractualmente a las empresas informáticas, se multiplican, ya que la recolección, organización y disposición de la información pueden resultar dañosas para las personas a las que se refiere, sea por su inadecuada manipulación, por su difusión no justificada o por su falsedad.

Los equipos constituyen, por sí, un arma importante para la comisión de una larga serie de delitos como la estafa, el espionaje político, industrial o comercial, etc. El uso de las técnicas puede ocasionar diversos daños: desde aquél que implica la posibilidad de realizar perfiles de la población por medio de la recopilación de datos tomados de los *test* ocupacionales. El aporte de datos no correspondiente a la realidad también puede resultar dañoso para quienes confían en ellos, la introducción de las máquinas por el deudor de una prestación en el cumplimiento de ella, puede también dar lugar a conflictos en los casos de mal funcionamiento que determine daños al acreedor, asimismo, los daños que pueden derivar de la programación defectuosa para el adquiriente que ve afectado su *hardware* o *software*. Son entonces diversas las situaciones de riesgo frente a las cuales se encuentra cualquier ciudadano que hace uso de estas tecnologías de información y comunicación. [8]

En el caso particular de Venezuela, puede decirse que este ciudadano cibernauta se encuentra indefenso, ya que se carece de una regulación de los múltiples problemas que motiva el otorgamiento de datos a través de los sistemas informáticos. Es necesario dictar normas regulatorias de la actividad informática y, en este ámbito, se deben incluir la regulación de los bancos de datos y sus posibilidades de exportación, importación, comercialización y difusión de la información en ellos contenida y la mayoría de las naciones lo contempla, incluso, como un derecho constitucional y consagrado a nivel de acuerdos internacionales, dándole el carácter de derecho fundamental.

Se ha dicho que los daños pueden ocasionarse entre personas vinculadas por una regulación voluntaria de sus conductas y en el desen-

volvimiento de tal relación o por personas no ligadas por vínculo contractual alguno; los primeros quedan sujetos a las disposiciones que rigen la responsabilidad en la órbita contractual; los segundos, en cambio, caen en la esfera extracontractual. En este caso hay varias situaciones que diferenciar:

Cuando se está frente a la actividad de comercio electrónico, generalmente la oferta se hace, o bien a través de un sistema cerrado (*correo electrónico o e-mail*) o bien se hace a través de un sistema abierto (*chat o mall virtuales*), que implican solicitar del cliente algunos datos. Ahora bien, dependerá del tipo de dato solicitado, el grado de responsabilidad por parte del oferente.

Partamos del supuesto de que el consumidor final ha otorgado datos personales y sensibles. Los datos personales son una categoría intermedia entre los nominativos sensibles y los anónimos, que no son identificables respecto de quien conciernen, pues si bien se refieren a una persona determinada, comprenden aspectos públicos de la personalidad del individuo (apellido, nombres, estado civil, estudios cursados, labores que desempeña, etc.).

El ingreso de este tipo de datos en los computadores debe ser libre, pero el *habeas data* deberá comprender el derecho de rectificación y de mantenimiento de la información en estado confiable.

Los datos de cualquier naturaleza —sensibles o personales— y cualquiera fuera el medio de recolección, lícito o no, que no se corresponda con la realidad, pueden importar una violación del derecho a la intimidad en cuanto desfiguran el perfil del sujeto referente.

Cuando existen datos falsos o erróneos, la culpa debe ser presumida, ya que el error la revela *in re ipsa*, pesando sobre quien incorporó el dato, la prueba de la excusabilidad del error, en tanto no hayan sido ilegítimamente recogidos. En tal supuesto, la invocabilidad de la propia torpeza lo impediría.

Debe aclararse que aun tratándose de un registro individual o particular del usuario, no excusa la responsabilidad del tenedor del dato erróneo si éste trasciende.

Tratándose de datos personales, pues es poco común que en materia de actividad de comercio electrónico se vean involucrados datos sensibles, en cuanto a la responsabilidad, excusando el hecho del tercero que ha suministrado el dato.

Por ejemplo, una empresa de informes para comerciantes, dice que una persona determinada es morosa, pues figura en sus registros en ese estado en una determinada casa de comercio; el dato no corresponde a la realidad. ¿Puede la empresa excusarse en razón de que la casa de comercio le había dado ese informe y no fue rectificado?

En principio, dentro de la legislación vigente, no encontramos posibilidad de rechazar la excusa. Se trata de una responsabilidad extracontractual subjetiva, en la que no es posible predicar culpa de la empresa, ya que el dato lo recibió de un tercero a quien es imputable el error. El sometimiento de la responsabilidad a una responsabilidad objetiva modificaría la solución, pues, el hecho del tercero es causa ajena que excusa.

En [8] considera que como la imputación es subjetiva, basta para excusar la responsabilidad, la demostración de que se tomaron todas las diligencias adecuadas para evitar el errado ingreso. La conclusión aparece como ineludible en el sistema jurídico actual de nuestro país. La prueba recaerá sobre el tenedor de la base de datos, pues el error hace presumir su culpa, quedando a su cargo la de la excusabilidad si pretende descargarla.

Otra situación que puede presentarse en el ámbito de la introducción de los datos es cuando hay fallas en el sistema, supongamos que el programa o *software* presenta errores o que el *hardware* no es eficiente.

Por ello, a veces la excusa que tienen los usuarios de computadoras es la de una falla en el sistema informatizado, por ejemplo, la carga del dato fue mal asumida o tomada por la lectora de la máquina. La alegación de la falla del sistema —sea del *software* o del *hardware*— implicaría la alegación del hecho de la cosa, de modo que si entre dañador y dañado no media vínculo contractual, importaría la confesión de que el daño no se debió al hecho personal, sino al hecho de la cosa. Tal afirmación es una confesión, en el más puro sentido técnico, pues comprometería su responsabilidad como dueño o guardián de la cosa.

En este contexto, puede decirse que la responsabilidad es un tema delicado, pero que debe precisarse en materia la actividad infor-

mática. En principio, debe aclararse que la actividad de comercio electrónico, si bien puede desarrollarse por correo, éste debe ser autorizado para ser recibido por el destinatario, pues de lo contrario estaríamos frente a lo que se denomina *spam*.

5.1. Tratamiento nacional e internacional en materia de privacidad e intimidad que se le dan a elementos tecnológicos, como el e-mail

En este sentido, vale hacer una breve referencia al *e-mail* y su protección nacional e internacional. El *e-mail* es uno de los medios tecnológicos a través de los cuales miles de millones de usuarios efectúan intercambio de información y transacciones múltiples. A nivel de la empresa u organización, existe una práctica frecuente en nuestros días, esta práctica es el monitoreo del contenido de los *e-mails* enviados y recibidos por sus empleados en sus lugares de trabajo. De igual forma, existen en los centros de comunicación e información una práctica de este monitoreo y, entonces nos preguntamos, ¿cómo proteger nuestra privacidad e intimidad como derechos fundamentales e independientes del mismo derecho de protección de los datos? Por ello, es necesario abordar cuál es el tratamiento que sobre esos datos y sobre la privacidad e intimidad se ha establecido en las distintas legislaciones.

Como se ha indicado a lo largo de este trabajo, la figura de protección de los datos posee una importancia para la región a nivel de sus constituciones, y con base a ello se han dictado algunas leyes en la materia en algunos países. Ahora bien, en torno a la privacidad e intimidad en la Constitución venezolana de 1999, se consagra el derecho a la intimidad, cuando establece:

> Artículo 60 de la Constitución Nacional: [...] La ley limitará el uso de la Informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.
> El reconocimiento de este derecho tiene su origen en el artículo 11 de la Convención Americana sobre Derechos Humanos, que establece: ‹Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, [...] o en su correspondencia, ni ataques ilegales a su honra o reputación›.

En este sentido, debe aclararse que la palabra *privacidad* sigue siendo un anglicismo en nuestro entorno. El Diccionario de la Real Academia de la Lengua Española aún no ha recogido dicho concepto. Sin embargo, la palabra es de uso corriente en el mundo jurídico y poco a poco se va diferenciando entre lo que es intimidad y lo que es privacidad.

El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. En este sentido, esta nueva generación de derechos que involucra la protección de los datos personales incluidos los datos sensibles (estado de salud, inclinación política, preferencias sexuales y conducta religiosa, entre otras), forman parte de lo que se denomina privacidad y nótese que se habla de la privacidad y no de la intimidad. Aquélla es más amplia que ésta, pues, en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona —el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo— la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan un perfil de la personalidad del individuo que este tiene derecho a mantener reservado.

Hoy el límite entre el tiempo y el espacio han desaparecido; las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, independientemente del lugar donde ocurrieron los hechos o por remotos que fueran éstos.

Precisamente, para evitar sean vulnerados estos derechos, es oportuno aclarar que en el caso de los trabajadores o empleados, para usar un término más amplio, se reconoce un derecho por parte del patrono a realizar el denominado monitoreo, pues los equipos, el software y la titularidad de las casillas de correo electrónico pertenecen, por lo general, a la empresa y, consecuentemente, el uso por parte del trabajador es una cesión de la empresa hacia éste, y en tal situación la empresa posee derecho a tal control.

Esto se considera correcto, pues tal control no implica entonces afectación alguna a la privacidad y a los derechos del trabajador.

Evidentemente, la postura empresarial más correcta y que evitaría cualquier discusión es la de notificar al trabajador o empleado que, tanto los equipos como el *software* o el *e-mail* suministrado por la empresa, es sólo y exclusivo para uso laboral, y que la empresa se reserva el derecho a dicho control. [4] A nivel jurisprudencial, se han producido los primeros pronunciamientos sobre el tema y, particularmente, en Argentina, en los cuales se ha debatido si el uso indebido del *e-mail* durante el horario de trabajo era causal de injuria que habilitaba el despido con causa.

Así, se consideró procedente el despido, entre otros casos, por la Sala X de la Cámara Nacional de Apelaciones del Trabajo de Buenos Aires (CNAT), en la causa «García Delia María del Rosario c/ YPF Yacimientos Petrolíferos Fiscales S.A. s/ despido» (13-08-2003); igual en el caso «V.R.I. c/ Vestiditos S.A. s/despidos (17-11-2003), la cual consideró que el correo electrónico provisto por una empresa posee las características de una herramienta de trabajo [...] que debe ser utilizada para el cumplimiento de la labor y no para fines personales.

De esta manera, ambas decisiones coincidieron en que «el hecho de utilizar las herramientas de trabajo para fines personales (y durante el tiempo de trabajo, cabe acotar) contraría deberes del trabajador contemplados en nuestro ordenamiento, tales como el de realizar el trabajo [...]; el de diligencia [...]; en especial, con dedicación adecuada a las características de su empleo y a los medios instrumentales que le provean, por lo que se acordó procedente el despido [11].

Por último, la Sala VII, en la causa «Pereyra, Leandro R. c/ Servicios de Almacén Fiscal Zona Franca y Mandatos S.A.» (27-03-03), afirmó que si la accionada no ha acreditado que haya dictado norma alguna escrita o verbal —sobre el uso que deberían hacer los empleados del correo electrónico de la misma, con el agravante de que despidió al actor sin hacerle ninguna advertencia previa—, ello torna injustificada la decisión de despido.

Ahora, lo que sí resultaría atentatorio para los derechos antes mencionados, es que en sitios de acceso a la red, pueda ser monitoreada la información que manejamos, y es lo que normalmente ocurre, de allí que recibimos correos no deseados o *spam*. Se nos brinda información de marketing que no requerimos, aparecemos en listas no conocidas, entre otros aspectos.

5.2. Algunas breves consideraciones sobre responsabilidad en el ámbito del comercio electrónico y la protección de los datos del consumidor final

El tema de la deslocalización, que no es otra cosa que la tercerización de servicios en otros países. Es así como grandes empresas tercerizan sus servicios de atención al cliente, procesamiento de datos y otros, contratando dichos servicios en otros países aprovechando las ventajas de los costos laborales, las diferencias horarias y las capacidades disponibles en otros países.

Para los clientes esto puede ser transparente, pero existe una preocupación real sobre el manejo de la información personal que los consumidores confían a las empresas que les prestan un servicio (financiero, por ejemplo). Es así que el tema de la protección de datos cobra importancia en el comercio internacional de servicios de información y en el comercio electrónico.

Varios países (últimamente los países miembros de la Organización de Cooperación y Desarrollo Económico - OECD) han desarrollado políticas específicas de protección de los datos de los consumidores y usuarios de servicios de telecomunicaciones (en el sentido amplio del término). Es así que la Comunidad Europea establece la Directiva sobre la privacidad y las comunicaciones electrónicas.

Dentro del marco del *Asia Pacific Economic Cooperation*, o Foro de Cooperación Económica Asia-Pacífico (APEC), también se viene trabajando en un marco internacional para la protección de datos que fluyen entre fronteras.

De lo anterior puede indicarse que, generalmente, en los códigos de conducta para la actividad de comercio electrónico se propone que las empresas que realicen publicidad o transacciones contractuales con consumidores a través de medios electrónicos de comunicación a distancia deberán:

1. Respetar la legislación vigente en materia de protección de datos personales.
2. Obtener los datos para su tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
3. Cancelar los datos cuando hayan dejado de ser necesarios

o pertinentes para dicha finalidad, o cuando lo solicite el titular en el ejercicio de su derecho de cancelación.

4. Respetar la privacidad de los usuarios, así como asegurar el secreto y seguridad de los datos personales, adoptando para ello las medidas técnicas y organizativas necesarias, habida cuenta del estado de la tecnología, la naturaleza de los datos y los riesgos a los que están expuestos.
5. Ayudar a educar al consumidor sobre cómo proteger su intimidad en los medios electrónicos de comunicación a distancia.
6. Abstenerse de utilizar los grupos de noticias, tablón de anuncios, foros o charlas para captar datos con finalidad publicitaria, salvo que dicha recogida se ajuste a las normas de obtención de datos establecidas en el presente Código.
7. Las empresas que se anuncian en Internet y que recaben, capturen y traten datos personales, deberán informar a los consumidores, mediante un aviso en su web, de dicho tratamiento. De esta forma, el consumidor podrá, si lo desea, ejercitar su derecho de oposición, tanto en lo que se refiere a la captación como al tratamiento y transferencia de sus datos.

Estos aspectos contribuyen a determinar la responsabilidad de las empresas que ofertan productos por la red, hay como una guía que facilita el tratamiento y la transmisión adecuada de los datos. Uno de estos códigos que sirven de referente es el Código Ético de Comercio Electrónico y Publicidad Interactiva, presentado públicamente el 28 de noviembre de 2002 y entró en vigor en enero del 2003. Ésta es su última versión, con las modificaciones introducidas entre noviembre de 2004.

6. Conclusiones

El derecho de protección de los datos es un derecho fundamental, pues está garantizado por el ordenamiento jurídico positivo, en la mayoría de los casos en su normativa constitucional, y que suelen gozar de una tutela reforzada como es el caso de los acuerdos internacionales.

En el contexto internacional se han adoptado una serie de instrumentos internacionales, convirtiéndose en la base de un sistema universal de promoción y protección de los derechos humanos, que va desde la Declaración Universal de Derechos Humanos, las Directrices para la regulación de los archivos de datos personales informatizados hasta la Declaración Americana de los Derechos y Deberes del Hombre, el Cuestionario para los Estados miembros de la OEA respecto a la legislación sobre el acceso a la información y la protección de datos personales, especialmente en forma electrónica. Este esfuerzo también se ha puesto al interior de los Estados, pues en sus constituciones se refleja la preocupación por recoger la figura del *habeas data*.

En cuanto a los métodos legales y técnicos, en cuanto a los primeros, se tiene las propuestas de autorregulación o celebración de acuerdos macro a nivel de varios países, donde se comprometen en torno a la protección de los datos; en cuanto a los segundos, se tienen: las plataformas de preferencias de privacidad, los agentes de *software* con protecciones de privacidad y los denominados infomediarios.

En el caso del *e-mail* a nivel laboral, se reconoce un derecho por parte del patrono a realizar el denominado monitoreo. Mientras que en el supuesto del acceso libre a Internet, sea monitoreada la información. En este caso, es una violación a nuestra intimidad y privacidad.

El *habeas data* consiste en proteger al individuo contra la invasión de su intimidad, ampliamente, su privacidad y honor, a conocer, rectificar, suprimir y prohibir la divulgación de determinados datos.

Cabe destacar que el tenedor o propietario de la base de datos que contiene datos de carácter personal, debe comportarse como un buen padre de familia.

Cuando el consumidor final ha otorgado datos personales y sensibles. El ingreso de este tipo de datos en los computadores debe ser libre, pero el *habeas data* deberá comprender el derecho de rectificación y de mantenimiento de la información en estado confiable.

Cuando existen datos falsos o erróneos, la culpa debe ser presumida, ya que el error la revela *in re ipsa*, pesando sobre quien incorporó el dato, la prueba de la excusabilidad del error, en tanto no hayan sido ilegítimamente recogidos; en tal supuesto, la invocabilidad de la propia torpeza lo impediría.

La imputación es subjetiva, basta para excusar la responsabilidad, la demostración de que se tomaron todas las diligencias adecuadas

para evitar el errado ingreso. La conclusión aparece como ineludible en el sistema jurídico actual de nuestro país. La prueba recaerá sobre el tenedor de la base de datos, pues el error hace presumir su culpa, quedando a su cargo la de la excusabilidad si pretende descargarla.

A veces la excusa que tienen los usuarios de computadoras es la de una falla en el sistema informatizado, por ejemplo, la carga del dato fue mal asumida o tomada por la lectora de la máquina. La alegación de la falla del sistema —sea del *software* o del *hardware*— implicaría la alegación del hecho de la cosa, de modo que si entre dañador y dañado no media vínculo contractual, importaría la confesión de que el daño no se debió al hecho personal, sino al hecho de la cosa. Tal afirmación es una confesión, en el más puro sentido técnico, pues comprometería su responsabilidad como dueño o guardián de la cosa.

Referencias Bibliográficas

Libros

Ayala, C.M. *Del amparo constitucional al amparo interamericano como Institutos para la Protección de los Derechos Humanos*. Caracas/San José: IIDH-Editorial Jurídica Venezolana, 1998.

Davarar, M. La Protección de Datos en Europa, principios, derechos y procedimiento, Madrid: Grupo Asnef Equifax, 1998

De Pablos, C., J López, S. Martín-Romo, S. Medina, A. Montero y J. Nájera. *Dirección y Gestión de los Sistemas de Información en la Empresa. Una Visión Integradora*. España: ESIC Editorial, 2.ª Ed., 2006.

Fernández, H. *Internet su problemática jurídica*. Argentina: Abeledo Perrot, 2001.

Flores, R. Amparo, *Habeas Corpus* y *Habeas data*. Buenos Aires: Editorial Montevideo, 2004.

Guerra V. *La Responsabilidad Civil Extracontractual por Productos en el Derecho Internacional Privado. Estudio Comparado*. Caracas: Publicaciones UCAB, 2002, 1.ª Ed.

Ortiz-O., R. *Habeas Data. Derecho fundamental y garantía de protección de los derechos de la personalidad (derecho a la información y libertad de expresión)*. Caracas: Editorial Fronesis, 2001.

Parellada, C. *Daños en la actividad judicial e informática desde la Responsabilidad Profesional*. Buenos Aires: Editorial Astrea/Depalma, 1990.

Pérez Luño, A. *Temas clave de la Constitución Española. Los derechos fundamentales*. Madrid: Tecnos, 2004, 8.ª Ed.

Puccinelli, O. *El Habeas Data en Indoiberoamérica*. Santa Fe de Bogotá: Editorial Temis, S.A., 1999.

Rico, M. *Comercio Electrónico Internet y Derecho*. Bogotá: LEGIS, 2005, 2.ª Ed.

Capítulos de libro

LIVELLARA, C. «Facultad de Contralor del Empleador vs. Derecho a la intimidad del trabajador». En *El Derecho del Trabajo Iberoamericano*. Libro Homenaje al doctor Baltasar Cavazos Flores. Lima: Editorial Juris Laboral, 2005, pp. 63-73.

Artículos de Revistas

FLORES, R. «Protección de datos personales de informes comerciales: Ley n.° 17838 de Uruguay». *Revista Electrónica de Derecho Informático*, n.° 084, julio 2005.

OLIVER, A. «Estrategias de protección de datos en el comercio electrónico». *Derecho y Tecnología*, julio-diciembre 2003, n.° 3, pp. 51-71.

Fuente Electrónica

Comité Jurídico Interamericano de la Organización de Estados Americanos (OEA), agosto, 2006. Disponible: www.oas.org

SAGUES, N. Subtipos de *habeas data*, nota a fallo, 1995. Disponible: www.alfa-redi.org, pp. 352-355.

Reportes

Comisión Mundial sobre la Dimensión Social de la Globalización por una Globalización Justa. Crear oportunidades para todos. Rendición OIT. Ginebra, febrero 2004, p. 36.

Organización de Estados Americanos, Corte Interamericana de Derechos Humanos, Secretaría de la Corte Interamericana de Derechos Humanos, San José de Costa Rica, 2005. Documentos Básicos en materia de Derechos Humanos en el Sistema Interamericano. Editorama, p. 326.

Diccionario

Diccionario de la Real Academia. Madrid: ESPASA, 1984, tomo I.