Cuestiones Jurídicas
Revista de Ciencias Jurídicas
de la Universidad Rafael Urdaneta
Vol. VI, N° 2 (Julio - Diciembre 2012)
ISSN 1856-6073

Protección de Datos frente a la publicidad en línea: Estudio Comparado* **

Gladys S. Rodríguez***

Resumen

Cuando los datos personales se obtienen de las denominadas fuentes de acceso público, parece ser lógico y válido disponer de tales datos para su posterior tratamiento informático. El objetivo general del artículo es comparar el régimen de protección venezolano con el español en lo referente a la protección de los datos que circulan por la red. Para ello, se realizó un estudio comparado de ambas legislaciones, un análisis jurisprudencial nacional y, lo expuesto por Paniza (2006), Hernández, (2005), Ortiz, (2001) y Ovilla, (2003). Dando por resultado el establecimiento de lineamientos para el tratamiento de los de datos frente a la publicidad en sitios electrónicos.

Palabras Clave: datos personales, régimen de protección, red, estudio comparado

* Recepción: 17/05/2012 Aceptación: 18/09/2012

** Avance de los Resultados del proyecto de Investigación intitulado: Plan Jurídico- Político en defensa y promoción a la libertad informática en Venezuela, registrado ante el CONDES bajo el No. CH-0152-12. Ponencia presentada en el marco del I Congreso Nacional de Derecho Patrimonial y Económico, celebrado los días 16 y 16 de marzo de 2012.

*** Abogada, Magister en Planificación y Gerencia de Ciencia y Tecnología, Doctora en Derecho y Postdoctora en Gerencia en las Organizaciones. Profesora Titular de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia. Investigadora acreditada en el programa de Estímulo a la Investigación (PEI, Nivel III), adscrita al Instituto de Filosofía del Derecho de L.U.Z. Correo electrónico: *stellagladys1@gmail.com.*

Data Protection versus online advertising: Comparative Study

Abstract

When personal data are obtained from public available sources known, it seems logical to have such data available for subsequent computer processing. The overall objective of this paper is to compare the Venezuelan protection regime with the Spanish one, regarding the protection of data flowing through the network. For this, we performed a comparative study of the two laws, one national jurisprudential analysis, and the one expound by (Paniza, 2006), (Hernandez, 2005), (Ortiz, 2001), (Ovilla, 2003). Resulting in the establishment of guidelines for the treatment of data from advertising on websites.

Key Words: personal data, protection system, network, comparative study

Introducción

Existe la idea de que cuando una información se obtiene de lo que alguien interpreta o califica como fuente de acceso público, es totalmente válido disponer de ella para su posterior tratamiento informático. En el caso de Venezuela ésta y otras situaciones de riesgo, sobre la obtención de información sobre los datos personales y el desconocer la finalidad del uso que se dará a estos datos, se acrecienta debido a la ausencia de legislación especial en la materia, contando sólo con una norma programática consagrada en la Constitución Nacional[1] y, algunas normas sectoriales sobre la protección para el tratamiento de los datos personales, que se indicarán más adelante,

[1] Constitución de la República Bolivariana de Venezuela. G.O. 36.860 del 30 de diciembre de 1999, Artículo 28.- Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley.

conjuntamente con unas sentencias del Tribunal Supremo de Justicia[1] (TSJ en adelante) . Sin embargo, no se trata de que el derecho de protección de datos trate de evitar que alguien sepa cosas sobre las personas, sino sobre todo de regular quién, cómo, y bajo qué condiciones puede procesar (recopilar, reelaborar y usar) aquella información que pueda vincularse con la persona, así como conceder a los ciudadanos ciertas facultades de control sobre sus datos. Pero lo que sí es fundamental es que si la sociedad moderna obliga a comunicar los datos personales, es lógico, que esta misma sociedad articule algunas condiciones o garantías para evitar el uso indebido con lo cual se pueda afectar a esos titulares de los datos.

En el presente artículo se tomará como referente el marco regulatorio español, por ser el régimen de protección más adelantado en Iberoamérica, además de contar con la normativa comunitaria que la fortalece significativamente. Por ello vale señalar, que en España, se tiene una legislación especial; por una parte está la Ley Orgánica de Protección de Datos Personales (LOPDP en adelante), que define qué ha de entenderse por fuentes de acceso público, señalando en concreto:

> "lo son - y sólo son éstas -, aquellas cuya consulta pueda ser realizada por cualquier persona, no impedida la misma por una norma limitativa, o, en su caso, sin más exigencia que el abono de una contraprestación; también lo son el censo promocional, los repertorios telefónicos (con los matices que su normativa propia contiene), así como también las listas de personas pertenecientes a grupos de profesionales (pero que contengan únicamente los datos del nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo). Igualmente se considerarán de acceso público los boletines oficiales y medios de comunicación"[2].

Ante esta última frase - los medios de comunicación - cabe preguntarse si Internet lo es. Siguiendo la doctrina española especial en la materia de

---

[1] Expediente No: 00-1797. Caso Insaca Sala Constitucional del TSJ de fecha 14 de marzo de 2001.Ponencia Jesús E. Cabrera. Sentencia No. 940, de la Sala Constitucional de fecha 21-05-2007, Caso: Asdrúbal Celestino Sevilla. Acción de Amparo. Ponencia Carmen Zuleta de Merchán y la Sentencia No. 1318, Expediente No. 04-2395, de la Sala Constitucional de fecha 04-08-2011, Caso: Recurso de Nulidad del "Decreto N° 1.526 con Fuerza de Ley de Reforma de la Ley General de Bancos y otras Instituciones Financieras". Ponencia Luisa Estella Morales Lamuño

[2] Art. 3 de la LOPDP, letra j.

protección de datos personales, la Agencia Española de Protección de Datos (AEPD) ha señalado:

> "No se considera que la procedencia de los datos recogidos en Internet sea la de fuente accesible al público, siendo necesario, por lo tanto, la obtención del consentimiento inequívoco, específico e informado del afectado para realizar tratamientos con sus datos personales publicados en Internet, aunque éstos se hayan publicado de forma que cualquier internauta pueda acceder a los mismos" (*www.adaptasoluciones.com* fecha de consulta 29-10-2011)

Por lo anterior, es claro que las direcciones que se obtienen - por ejemplo - usando un programa tipo *Spider*[1] (del inglés, araña) que de forma automática rastree la Red, y recopile direcciones e-mail, no sería legal usar tales direcciones. Lo mismo ocurriría aunque no se hubiese usado dicho tipo de software, sino que se hiciere de forma manual, no automática. Evidentemente, si antes de usar dichas direcciones se solicita el permiso de su titular para remitirle por ejemplo un boletín, siguiendo y aplicando para tal fin los criterios ya expuestos acerca de la interpretación que sobre este hecho efectúa la AEPD, se estará - legalmente "inmaculado" (Hernández, 2005).

En este sentido, se puede ser víctima no sólo cuando a través de la cuenta de e-mail alguna persona o institución, con la aplicación de este tipo de programa en red, recibe correos no deseados o no solicitados, sino que pueden alojarse en su equipo o correo algunos archivos maliciosos. Situación muy común cuando se reciben anuncios publicitarios, por ello, se coincide con (Paniza, 2006: 24-25), cuando señala: "… las empresas de marketing directo pueden verse favorecidas según se encuentren en un lugar o en otros dependiendo de su normativa y obviamente estarán mucho más

[1] (Robot-Web, araña, *bot, web crawler).* Programa que recorre la WWW y recoge páginas web, visitando los enlaces que tiene de forma automática. Suelen utilizarlo los grandes buscadores para dar de alta (indexar) las páginas y luego poder buscar en ellas. Diccionario de informática: *www.alegsa.com.ar* (Fecha de Consulta 01-10-2012). Uno de los métodos más comunes e ilegales a la hora de captar cuentas de correo de manera indiscriminada, es el uso de programas araña o Crawlers. Estos son de fácil adquisición e instalación y realizan verdaderas hazañas a la hora de captar cuentas de correo, teléfonos y otros datos personales de urls en Internet. Lo importante de estos robots de captación de datos radica en conocer que su uso es totalmente ilegal y sancionado por las agencias encargadas de proteger los datos. Pérez, A. 2010 "Crawlers, programas araña en email marketing. LOPD, LSSICE y AEPD". En: *www.teenvio.com.es* (Fecha de Consulta 1-10-2012)

cómodas donde la regulación sea más permisiva. Siendo la armonización en este caso una cuestión fundamental".

A lo largo del siguiente trabajo se comparará el régimen de protección venezolano con el régimen de protección español, siendo este último un referente para mejorar el sistema de protección nacional; se expondrá algunos aspectos sobre publicidad y comunicaciones comerciales en la red; se describirá el proceso de creación y utilización de bases de datos con fines publicitarios, indicando los límites para los responsables de las bases de datos; se establecerán algunos lineamientos para el tratamiento de los datos por parte de los responsables de sitios electrónicos donde se recogen los datos de los consumidores, especialmente cuando se hallan frente a la actividad de publicidad y; finalmente, se expondrán los principios que deben regir la protección de datos de carácter personal en el medio electrónico como estrategias de protección.

1. Algunas consideraciones previas

En el desarrollo de este trabajo es necesario hacer algunas precisiones previas: En primer lugar, con referencia al ordenamiento legal, se tomará como referente a la legislación especial en la materia de protección de datos de España, pues como se indicó en Venezuela, no hay ley especial, aunque se hará referencia a los casos regulados específicamente por la norma nacional, cuando así sea pertinente. En segundo lugar, resulta oportuno señalar cuáles son las principales instituciones competentes tanto en España como en Venezuela en la materia de protección de datos y, así establecer cómo se encuentra estructurado el régimen de protección en ambas naciones. Y, en tercer lugar, exponer el tratamiento otorgado en ambos países sobre la conservación de los datos.

En primer término, Venezuela forma parte de la Red Iberoamericana de Protección de Datos (*http://www.redipd.org* Consultada 12-10-11) [1] y, cuenta

[1] La Red Iberoamericana de Protección de Datos (RIPD), surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, con la asistencia de representantes de 14 países iberoamericanos. La RIPD se constituye como una respuesta a la necesidad de fomentar, mantener y fortalecer un estrecho y constante intercambio de información, experiencias y conocimientos entre los Países Iberoamericanos, a través del diálogo y colaboración en materia de protección de datos de carácter personal. La RIPD se encuentra abierta a todos los países iberoamericanos que deseen promover y ejecutar iniciativas y proyectos relacionados con esta materia. Ver *www.redipd.org* Fecha de consulta 12-10-11.

con un régimen de protección que descansa en la máxima norma como lo es la Constitución venezolana de fecha 15 -12-1999, específicamente en el Art. 28, ya referido; respetando lo acogido por la Declaración Universal de los Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos. La legislación nacional comprende siete normas sectoriales vigentes y un Decreto No. 9051 publicado en Gaceta Oficial N° 39.945 de fecha 15 de junio de 2012 que entrará en vigencia a los dos años a partir de la fecha de su publicación. Las normas sectoriales aplicables por la materia, son : Ley de Registro de Antecedentes Penales del 31-08-1979 (Arts. 6 al 8); Ley sobre Protección a la Privacidad de las Comunicaciones del 16-12-1991; Ley Orgánica para la Protección del Niño, Niña y Adolescente del 07-12-2007 (Arts. 65 al 68); Ley Especial contra Delitos Informáticos del 30-10-2001 (Arts. 20 al 30); el Decreto con fuerza y rango de Ley para la Defensa de las Personas en el Acceso a los Bienes y Servicios del 01-02-2010 (Arts. 8, 37 y 38), el Decreto con fuerza y rango de Ley de la Función Pública de Estadística del 09-11-2001 (Arts. 5 al 26), cabe señalar que esta última ley recoge algunos principios internacionalmente establecidos en materia de protección de datos, y el Decreto con fuerza de Ley Nº 1204 , del 10 de febrero de 2.001, Sobre Mensajes de Datos y Firmas Electrónicas (Arts. 4, 5 y 7). En cuanto al Decreto No. 9051, en sus (Arts. 20, 22, 32, 34, 43 al 47), hace referencia a la interoperabilidad como interés público, el acceso al intercambio de datos, información y documentos, a la disponibilidad y acceso de los servicios, la seguridad de tales servicios, la certificación electrónica, las características de los datos, información y documentación y, el uso de los datos, información y documentos. De igual modo, existen dos Proyectos de ley: Proyecto de Tecnología de la Información y el Proyecto de Ley de Protección de Datos y Habeas Data en Venezuela, desde el año 2004.

En segundo término, desde el punto de vista institucional, existen cinco órganos con incidencia en la materia de protección de Datos: Consejo Nacional Electoral, la Defensoría del Pueblo, la Superintendencia de Servicios de Certificación Electrónica, Instituto para la Defensa de las Personas en el Acceso a los Bienes y Servicios, Instituto Nacional de Estadística, éste último es un órgano público venezolano encargado de ser un instituto estadístico de referencia nacional e internacional, con alta capacidad técnica y liderazgo para ejercer la rectoría del Sistema Estadístico Nacional, como se desprende de su filosofía de gestión y, que por tanto maneja un gran volumen de datos, cuyo referente más próximo fue el Censo del 2011. Así mismo, existen los órganos jurisdiccionales ante quienes se presenta la acción de *habeas data*:

en el caso venezolano son los Tribunales de Primera Instancia del país, a partir de la Ley Orgánica del Tribunal Supremo de Justicia de fecha 01-10-2010, que establece el procedimiento de habeas data en su Capítulo IV del Habeas Data (arts. 167 al 178), pues anteriormente la competencia para conocer de esta acción era atribuida a la Sala Constitucional del Tribunal Supremo de Justicia, esto de acuerdo a lo que establecía la Sentencia de la Sala Constitucional en el Caso Insaca[1] . Y en cuanto a Organizaciones No Gubernamentales (ONG) con especial referencia a los temas de Derechos Humanos se tienen: la Federación Venezolana de la Asociación de Consumidores y Usuarios, la Alianza Nacional de Usuarios y Consumidores (ANAUCO) una asociación civil sin fines de lucro, conjuntamente con El Programa Venezolano de Educación-Acción en Derechos Humanos (Provea) una ONG especializada en la defensa y promoción de los derechos económicos, sociales y culturales. Y aunque parece existir una institucionalización para la protección de los datos personales, lo cierto es que se regula de

[1] "En primer lugar corresponde a esta Sala decidir acerca de su competencia para conocer la consulta a que se refiere el artículo 35 de la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales, de la sentencia dictada por la Corte Primera de lo Contencioso Administrativo el 14 de abril de 2000, al conocer ésta en primera instancia de la acción de habeas data interpuesta el 21 de marzo de 2000 por Carlos Julio González Siabra y María Carolina González Prado, en su carácter de apoderados la empresa INSACA, contra las actuaciones del Director de Drogas y Cosméticos de la Dirección General Sectorial de Contraloría Sanitaria del Ministerio de Salud y Desarrollo Social, contenidas en el memorándum Nº 097 de 2 de septiembre de 1999, respecto de lo cual observa esta Sala que la acción de habeas data como acción autónoma no ha sido aun desarrollada por la ley, no obstante lo cual, con fundamento en las previsiones contenidas en el artículo 27 de la Constitución de la República Bolivariana de Venezuela, considera esta Sala que la protección de los derechos constitucionales consagrados en los artículos 28, 58, 60 y 143 eiusdem, puede ser ejercida mediante la acción de amparo. Señala esta Sala que en sentencias de fecha 20 de enero de 2000, casos Emery Mata Millán y Domingo Gustavo Ramírez Monja, al determinar los criterios de distribución de competencia aplicables a la acción de amparo a la luz de los principios y preceptos contenidos en la vigente Constitución, quedó asentado que corresponde a la Sala Constitucional del Tribunal Supremo de Justicia conocer de las apelaciones y consultas a que se refiere el artículo 35 de la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales, de las sentencias dictadas por la Corte Primera de lo Contencioso Administrativo, cuando ella conozca de acciones de amparo en primera instancia, como ocurre en el presente caso". Sentencia Sala Constitucional 14-03-2001.

manera casuística, quedando el ciudadano en un estado de indefensión, si no está en algunas de las situaciones reguladas sectorialmente.

En tercer término, debe determinarse cuáles son los datos que deben ser conservados, para (López, 2008: 74), "los datos que deben ser conservados son los datos de tráfico, localización y otros datos necesarios para identificar al titular o usuario registrado, pero en ningún caso incluyen datos relativos al contenido de las comunicaciones". La norma española[1], en el artículo en el que detalla los datos concretos que quedan sujetos a la obligación de conservación, ha reproducido con exactitud, el listado contenido en la Directiva 24/2006/CE. Este listado comprende los datos necesarios para: 1. Rastrear e identificar el origen y el destino de la comunicación; 2. Determinar su fecha, hora y duración; 3. Identificar el tipo de comunicación y el equipo de comunicación utilizado; y 4. Identificar la localización en los casos de equipos de comunicación móvil. En cuanto a qué tipo de datos serán conservados en la legislación nacional no se hace referencia a esta categoría, sino que se menciona su tiempo de conservación en forma general. En cuanto al período de conservación de datos, mientras que la Directiva 24/2006/CE se limita a establecer que el período de retención no deberá ser inferior a seis meses ni superior a dos años, dejando al arbitrio del legislador español la determinación del plazo concreto dentro de los límites señalados, otro aspecto plantea la Ley de Conservación de Datos española en su art. 5 que establece que la obligación de conservación cesará a los doce meses computados desde la fecha en que se haya producido la comunicación, aunque reglamentariamente y previa consulta a los operadores, se podrá ampliar o reducir el plazo de doce meses para determinados datos hasta un máximo de dos años o un mínimo de seis meses. En el caso de Venezuela la Ley de Indepabis [2] establece en su artículo 39, parte final, en el Capítulo sobre

[1] Ley 25/2007 de Conservación de Datos de España de fecha 18-10-2007, se encarga de regular la conservación de los datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

[2] Ley Para La Defensa de las Personas en el Acceso a los Bienes y Servicios, Gaceta Oficial de La República Bolivariana de Venezuela Número 39.358, Caracas Lunes 1 de Febrero de 2010, cuyo Objeto es la defensa, protección y salvaguarda de los derechos e intereses individuales y colectivos en el acceso de las personas a los bienes y servicios para la satisfacción de las necesidades, estableciendo los ilícitos administrativos, sus procedimientos y sanciones; los delitos y su penalización, el resarcimiento de los daños sufridos, así como regular su aplicación por parte del Poder Público con la participación activa y protagónica de las comunidades, en resguardo de la paz social, la justicia, el derecho a la vida y la salud del pueblo.

Comercio Electrónico: "Las proveedoras o proveedores estarán obligados a mantener un registro electrónico con su respaldo de seguridad respectivo, por un lapso de cinco años o en su defecto durante el tiempo que establezcan las leyes respectivas, una vez realizada la compra", lo cual resulta favorable, siendo razonable el tratamiento por ser en protección del consumidor. Y por su parte la jurisprudencia del TSJ[1] plantea el principio de la temporalidad o conservación de los datos y que la misma se extiende hasta el logro de los objetivos para las cuales han sido elaborados, vale decir, que justificaron su obtención y tratamiento.

2. Algunos conceptos básicos

De igual manera, es necesario delimitar algunos conceptos para los fines del trabajo, tales como: datos personales, dirección electrónica y correspondencia publicitaria, que son recurrentes a lo largo del tema de la protección de los datos.

En primer lugar, por dato debe entenderse "Hecho, concepto, instrucción o caracteres, que se expresa por sí mismo, representado de una manera apropiada para que sea comunicado transmitido o procesado por seres humanos o por medios automáticos, y al cual se le asigna o se les puede asignar un significado" (Art. 4 Decreto venezolano No. 9051). Por su parte el Diccionario de la Real Academia Española define dato como: "Información dispuesta de manera adecuada para su tratamiento por un ordenador" y, personal como "Perteneciente o relativo a una persona" (En: *www.rae.es* Consultada 04-10-12). En segundo lugar, dirección electrónica es un "Sistema de comunicación personal por ordenador a través de redes informáticas" (En: *www.rae.es* Consultada 04-10-12) o "Correo enviado a través de medios electrónicos, inicialmente se trataba de mensajes de texto, actualmente se puede enviar cualquier tipo de información" (Rico, 2005: 326). Y, en tercer lugar, la correspondencia publicitaria es el "Envío y divulgación de noticias o anuncios de carácter comercial para atraer a posibles compradores, espectadores, usuarios" (En: *www.rae.es* Consultada 04-10-12). De lo anterior se puede afirmar que tanto el concepto de dato personal como el de correo o dirección electrónica, pueden ser incluidos en

[1] (Sentencia No. 1318, de fecha 04-08-2011, Ponencia Luisa Estella Morales L. Caso Nulidad del Decreto No. 1.526 con fuerza de Ley de Reforma de la Ley General de Bancos y Otras Instituciones Financieras". En: *www.tsj.gov.ve/decisiones/scon/Agosto/1318-4811-2011-04-2395.html*. Fecha de consulta 29-09-2012)

el concepto de mensajes de datos, que de acuerdo al Decreto No. 1.024, con rango y fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas venezolano, es "Toda información intelegible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio" (Art. 2). Y resultan ambas categorías: dato y dirección electrónica, elementos personales porque cualquier dato o información (correo, fecha de nacimiento, nombre, dirección, entre otros), aun cuando estén aislados, identifican, constituyen un atributo o le añaden una cualidad al sujeto, que le merece un tratamiento digno y de salvaguarda. Ahora bien, la correspondencia publicitaria, no hace alusión a un dato personal, pero la recepción de la publicidad puede generar una recolección de datos personales, que permiten crear perfiles de usuarios o consumidores y, que pasa por desapercibido debido al mensaje subliminal y casi inofensivo del anuncio publicitario[1].

Una vez delimitado las consideraciones conceptuales y la estructura del artículo se procederá a desarrollar sus objetivos.

3. Algunos aspectos sobre Publicidad y Comunicaciones Comerciales

Constantemente los ciudadanos transfieren información, datos personales y patrimoniales, en fin intercambian mensajes de datos, bien sea como usuarios o consumidores, como proveedores o simples ciudadanos en actuaciones ante la administración pública o en el ámbito privado. Y es en éste último escenario donde surge la mayor inquietud ante la carencia de normativa especial que atienda a la protección del titular de dichos datos personales. Continuamente se es destinatario o proveedor de lo que Rico (2005: 6) denomina, "los servicios de la información que ofrecen múltiples posibilidades en el ámbito empresarial y comercial para el suministro de diversas actividades en línea… servicios de empresa a empresa, de empresa a consumidores, suministro de información, servicios educativos, comunicaciones comerciales, adquisición de mercancías, servicios profesionales, servicios de entretenimiento, banca electrónica y otros servicios como turismo, seguros, transporte y viajes, entre otros". Y uno de los escenarios de la red de redes donde se genera un creciente intercambio de datos, es cuando se realizan actividades de comercio electrónico[2] y, si se habla de

[1] Puede consultarse Rodríguez, G (2012) "Riesgos del consumidor electrónico en las prácticas publicitarias" En: **Revista de Derecho**, Universidad del Norte, 37:254-282, 2012.

[2] En un sentido amplio, se dice que el comercio electrónico, es "…. Todo inter-

comercio electrónico, según Huet y Maisl (1998:61) "debe hablarse de inmaterialidad y de fugacidad de información". En este sentido, aun cuando es evidente, no parece actualmente ser reconocido , que el consumidor en el comercio electrónico, como afirma Ortiz (2001), tiene por una parte el derecho fundamental de información y, por otra a que la información que ofrece a través de estos sitios web, sea objeto de protección, especialmente aquellos datos de carácter personal, aspecto que parece medianamente abordado en Venezuela, dado el marco legal señalado y las instituciones de gobierno y no gubernamentales involucradas. Sin embargo, como afirma Lorenzini (2000), la información que reciben los consumidores y usuarios sobre los productos y servicios es adquirida a través de soportes publicitarios y la información sobre diversos aspectos, que obligatoriamente debe proporcionar el proveedor, también se logra a través de la publicidad, siendo entonces el fenómeno publicitario esencial para formar el llamado, por este autor, el *derecho del consumo.* En este sentido, es desde el momento mismo de la publicidad, una de las actividades de comercio electrónico, que el consumidor debe tener garantía de la protección de los datos que ofrece o suministra en línea, a fin de profundizar en la descripción del producto o servicio o para en lo sucesivo recibir información publicitaria sobre otros bienes y servicios de su posible interés.

Esta inmaterialidad y fugacidad de la información que sostienen Huet y Maisl (1998), pueden crear algunos conflictos entre los proveedores de servicios y los clientes, y sólo puede verse solventada ante la generación de confianza, por lo que resulta imperante un entorno técnico-legal adecuado para el comercio electrónico, ya que no sólo se produce en este entorno, un incremento de intercambios mercantiles por Internet, sino que son miles o

cambio de datos por medios electrónicos, este relacionado o no con la actividad comercial en sentido estricto" Martínez, A. 1998. **Comercio electrónico, firma digital y autoridades de certificación.** Madrid. Civitas. p. 25. En este sentido, el concepto de comercio electrónico no se refiere únicamente a las operaciones comerciales electrónicas estrictamente consideradas (la compraventa de bienes o la prestación de servicios), sino que abarca dentro de ella, las negociaciones previas, las actividades ulteriores relacionadas y otros no remunerados por su destinatario como aquello que consiste en ofrecer información en línea, es decir, anuncios o correspondencia publicitaria. En España, el comercio electrónico también ha sido definido en sentido amplio, entendiéndose por tal, "cualquier forma de transacción de datos sobre redes de comunicación como Internet" En: Estudio de la situación actual del comercio electrónico en España, Informe del Ministerio de Fomento, mayo de 1999. *www.sgc.mfom.es/satcomunicación* (Fecha de Consulta 02-10-11)

millones los datos personales que circulan por ella. Es necesario además promover un entorno competitivo en el cual el comercio electrónico pueda crecer y asegurar la protección adecuada de los objetivos de interés público como son el derecho a la intimidad, los derechos de la propiedad intelectual, la prevención del fraude, la seguridad nacional y la protección al consumidor (Ovilla, 2003: 2).

Para lograr una mejor comprensión, si la actividad publicitaria, como parte del comercio electrónico, en su sentido amplio, como fue definido antes, implica según La Real Academia Española "…. la divulgación de anuncios de carácter comercial para atraer a posibles compradores, usuarios, etc" (*www.rae.es* Consultada 02-10-12), pareciera que todo vale en esta labor de divulgación comercial y, no es así pues encuentra limitaciones en la materia de protección de datos. El tratamiento de datos con fines de publicidad y de prospección comercial debería establecer dos únicas posibilidades de procedencia de los datos a utilizar: 1. Los datos que sean facilitados por los grupos interesados u obtenidos con su consentimiento y 2. Los datos que figuren en fuentes accesibles al público, como lo afirma entre otros Álvarez (2006), con base a la LOPDP[1]. En consecuencia, se puede permitir el envío de comunicaciones comerciales a aquellos usuarios que: a) previamente lo hubieran autorizado, b) lo hubieran solicitado de forma expresa o, c) cuando con ellos exista una relación contractual previa, en cuyo caso, se podrá enviar publicidad sobre productos o servicios similares a los contratados por el cliente[2]

En todo caso, en cada envío mediante correo electrónico se debe:

---

[1] La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPDP), es una Ley Orgánica española que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. Su objetivo principal es regular el tratamiento de los datos y ficheros, de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan.

[2] Desde el punto de vista de Marketing y de las herramientas de comunicación comercial de las que dispone la empresa para comunicarse con su público objetivo, cuando la organización envía un mensaje publicitario "personal a un receptor "identificable", con la posibilidad de medir la "respuesta" de éste último, ya no se estaría ante publicidad (comunicación comercial impersonal) sino de Marketing Directo.

a) Incluir la palabra "publicidad" al inicio del mensaje (no es necesario incluirla en el asunto)

b) Incluir una cláusula que podría venir a decir: ¿Ha recibido este correo porque es usuario registrado de "la Empresa X" y ha aceptado recibir comunicaciones electrónicas relacionadas con nuestros productos o servicios. Si desea revocar dicho consentimiento devuelva este correo indicando en el asunto del mensaje: Baja correo/ y procederemos a eliminarlo de la lista de distribución.

c) Asimismo, se recomienda que se incluya en el pie del correo lo siguiente: "Este correo se dirige a: _____ @cantv.net" Con ello se evitan posibles reclamaciones de terceros a quienes les podría llegar el correo reenviado y,

d) Es importante incluir un enlace directo a la "Política de Protección de Datos" de la empresa.

De lo anterior, se puede precisar que existen algunas excepciones a estos códigos de conducta en el entorno de comunicaciones comerciales electrónicas y, para ello se seguirá lo establecido por la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico de España (en adelante LSSICE)[1]:

> 1. La excepción siempre presente al sistema referido es: La regla general de la necesidad de consentimiento previo para el envío de comunicaciones comerciales encuentra su excepción cuando existe una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente. Así lo consagra el art. 21 de la LSSICE.

a) En este mismo sentido, siguiendo a Paniza (2006), también se debe tener en consideración la relación contractual previa: Parece que tiene que haberse perfeccionado un contrato entre las partes para que entre en juego la excepción. Sin embargo, hay otras cuestiones problemáticas relacionadas con el tiempo y con el modo, respectivamente, de esta "relación contractual previa". Y por ello, se pregunta: ¿puede tratarse de un contrato celebrado hace mucho tiempo?, ¿dónde está el límite temporal? Y por otra parte, ¿tiene

[1] Ley 34/2002 de fecha 11 de julio de 2002 que ha sido la encargada de modificar los preceptos clásicos dedicados al momento de la perfección del contrato a distancia

que ser necesariamente una venta celebrada a través de medios electrónicos o puede haberse llevado a cabo con persona física siempre que se hayan obtenido estos datos?

b) Algunos autores como Ortiz (2001), Chen,(2010) y Ovilla (2003) con los cuales se comparte su opinión, se refieren a los datos obtenidos de "forma lícita" y, han ratificado que tanto la dirección de correo electrónico como el número de teléfono móvil pueden considerarse datos de carácter personal, pues se trata de información dispuesta para ser almacenada, transferida o intercambiada a través de un ordenador y que le pertenece a una persona o lo relaciona con ella, como se explicara *supra*. Pero estos datos deben haberse obtenido de forma lícita, es decir bien a través de fuentes accesibles al público o que se haya obtenido el consentimiento del cliente o consumidor o como se acotó antes, conseguir el dato aunque no medie el consentimiento del destinatario porque los datos provienen de una relación contractual previa y se vaya a utilizar para las finalidades concretas como lo establece el art. 21.2. LSSICE, a menos que sean incompatibles con aquellos fines para los que hubieran sido recogidos (art. 4.2. LOPDP). También Venezuela contempla por vía jurisprudencial principios protectores; el principio de autonomía de la voluntad y el principio de finalidad y calidad, son algunos de ellos y pertinentes en estos casos de ofrecer consentimiento[1]. En este sentido, si hay consentimiento no hay duda ni problema para el tratamiento

[1] **El principio de la autonomía de la voluntad**. Lo cual comporta la necesaria existencia de un consentimiento previo, libre, informado, inequívoco y revocable para el uso o recopilación de datos personales. También deriva del presente principio, el deber de informar al interesado previamente o al tiempo de recolección de datos, elementos como la identidad del responsable de los mismos, los fines para los cuales son recolectados y el modo en que podrá hacer efectivos su derecho a la autodeterminación, así como de cualquier otra información necesaria para garantizar el derecho a la protección de datos personales. - **El principio de finalidad y calidad**. La recopilación de datos personales debe responder a finalidades, motivos o causas predeterminadas, que no sean contrarias al ordenamiento jurídico constitucional y sectorial, lo cual se constituye además en un requisito necesario para obtener un consentimiento válido de conformidad con lo indicado en el principio de autonomía de la voluntad. Así, el principio de finalidad comporta igualmente la necesaria proporcionalidad que debe existir en la obtención sólo los datos que resulten adecuados, pertinentes y no excesivos en relación con las finalidades para los cuales se requieren. (Sentencia No. 1318, de fecha 04-08-2011, Ponencia Luisa Estella Morales L. Caso Nulidad del Decreto No. 1.526 con fuerza de Ley de Reforma de la Ley General de Bancos y Otras Instituciones Financieras". En: *www.tsj.gov.ve/decisiones/scon/Agosto/1318-4811-2011-04-2395.html*, Fecha de consulta 29-09-2012)

de los datos, pero sí que se plantea una cuestión interesante respecto a la forma en que debe presentarse este consentimiento: es el caso de que se incluyera en un clausulado de condiciones generales, se pregunta: ¿sería esta manifestación de voluntad libre, inequívoca, especifica e informada cuando se trata del clausulado de unas condiciones generales? Parece que la respuesta tendría que ser negativa.

c) Productos o servicios similares a los que inicialmente fueron objeto de contratación con el cliente: Se exige que los datos se hayan obtenido en una relación previa y se utilicen para publicitar "productos o servicios similares", no valdría cualquier producto de la misma, sino productos o servicios (de características) similares. Se establece que no se trata de un concepto fácil de aplicar en la práctica y debe enfocarse desde la perspectiva del destinatario, no desde la del vendedor. Además debe tenerse en cuenta lo que razonablemente puede esperar el destinatario.

d) La misma empresa: es necesario que los datos los utilice la "misma empresa" (art. 21.2 LSSICE), sea persona natural o persona jurídica y que después sea esa misma "persona natural o jurídica", no un tercero quien utilice los datos. Pero ¿qué ocurre cuando se trate de un grupo de empresas?, ¿quién puede utilizar los datos recogidos en el marco de una relación contractual?. Parece que, en principio, sería la que realmente ha sido parte en ese contrato.

e) Procedimiento sencillo y gratuito de oposición: En la práctica, algunas empresas basan el ejercicio de este derecho en el envío de un escrito a la dirección física de la empresa, llamando a un teléfono, eso sí, gratuito, o entrando en una determinada página web. ¿Cumplen estas formulas con los requisitos del procedimiento "sencillo y gratuito"?. En la Comunicación de la Comisión Europea sobre las comunicaciones comerciales no solicitadas o *spam* establece que el nuevo régimen sobre comunicaciones comerciales tiene como norma fundamental el que todos los mensajes electrónicos deben mencionar una dirección de respuesta válida donde el abonado pueda pedir que no se le envíen más mensajes. ¿Se cumple en el caso de mensajes SMS a través del teléfono móvil? ¿Cómo podría cumplirse? Parece que los aspectos legales y técnicos del tema confluyen necesariamente; una actuación conjunta aportaría soluciones eficaces.

Además, agrega Paniza (2006), en el plano temporal, este procedimiento sencillo y gratuito de oposición debe ofrecerse tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que se le dirija al consumidor. Si bien en el caso del correo electrónico es bas-

tante factible, la cuestión que se plantea es: ¿Se cumple esto en los mensajes SMS?. Con carácter general, no. ¿Podrá suponer esta exigencia una carga demasiado elevada para la empresa en cuestión? ¿Qué vías técnicas pueden proponerse para la aplicación real de esta normativa sea un hecho?

Otro aspecto a considerar y el cual requiere de lineamientos es el caso de los denominados programas espías que llegan al computador, por ejemplo, cuando se publicita un software gratuito, después de que el usuario haya aceptado, sin previa lectura en la mayoría de las ocasiones, las condiciones de uso que se facilitan en inglés, las preguntas que surgen son: ¿se cumple lo manifestado bien por el TSJ, en cuanto al principio de finalidad y calidad o por lo establecido en la Ley de la Función Pública de Estadística nacional, cuando en su artículo 11, dispone:

> "Los datos de carácter personal sólo se podrán recolectar y someter a tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y la finalidad determinada, explícita y legítima para la que se hayan obtenido.
>
> Estos datos no podrán usarse para finalidad distinta de aquella para la cual han sido recogidos…."

Similar disposición está contemplada por el artículo 22.2 de la LSSICE, referente a que:

> "cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, **informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad**[1], ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito".

En este caso, ¿Se cuenta con el consentimiento del usuario?, Muchas veces el usuario carece de un software específico que le permita darse cuenta de que están captando información suya.

Como puede apreciarse, tales excepciones generan interrogantes, algunas con respuestas otras que deberán ser debatidas hasta acordar medidas prudentes.

---

[1] Destacado nuestro.

4. Creación y utilización de bases de datos de carácter personal con fines publicitarios: Limites

4.1. Creación de bases de Datos de carácter personal con fines publicitarios

En cuanto a la vida privada de los consumidores, existe a nivel mundial una preocupación para su protección. La Organización de Cooperación para el Desarrollo Económico (OCDE), publicó en 1980 sus líneas directivas relativas a la protección de la vida privada y los flujos transfronterizos de informaciones nominativas. De manera general, se recomienda a los países miembros que supriman o eviten crear obstáculos injustificados a los flujos transfronterizos de datos personales, bajo el pretexto de una protección de la vida privada[1] . Estas Líneas directivas enumeran algunos principios fundamentales que se pueden aplicar a un nivel nacional: principio de limitación en materia de recopilación de datos (obtención por medios lícitos); principio de la calidad de los datos, principio de la especificación de la finalidad de la recopilación, principio de su utilización, principio de transparencia y, finalmente principio de la participación individual (derecho de acceso y rectificación). Venezuela por su parte en reciente sentencia del TSJ[2], ha ratificado algunos principios, a saber: 1.El principio de la autonomía de la voluntad. 2.- El principio de legalidad. 3.- El principio de finalidad y calidad. 4.- El principio de la temporalidad o conservación. 5.- El principio de exactitud y de autodeterminación 6.- El principio previsión e integralidad 7.- Principio de seguridad y confidencialidad. 8.- Principio de tutela. 9.- Principio de Responsabilidad. Sin embargo, queda pendiente lo de acceder a un procedimiento gratuito, sencillo no sólo en lo atinente a la recogida de los datos sino en cualquier momento de la navegación por la red que implique transferencia de datos.

Por otra parte, en la legislación española, concretamente LOPDP, autoriza la creación de bases de datos de titularidad privada… cuando tal creación resulte necesaria…. y siempre que se respeten las garantías que

---

[1] Punto 2 de las Líneas directivas relativas a la protección de la vida privada y a los flujos transfronterizos de datos personales.

[2] (Sentencia No. 1318, de fecha 04-08-2011, Ponencia Luisa Estella Morales L. Caso Nulidad del Decreto No. 1.526 con fuerza de Ley de Reforma de la Ley General de Bancos y Otras Instituciones Financieras". En: *www.tsj.gov.ve/decisiones/scon/Agosto/1318-4811-2011-04-2395.html*. Fecha de consulta 29-09-2012)

la propia ley establece para la protección de las personas. En el caso de la normativa venezolana, se establece en la Ley de la Función Pública de Estadística en su artículo 38[1], la creación de bases de datos pero de carácter público, dado la naturaleza de la norma.

En el caso español, como resulta evidente, deberán cumplirse las exigencias generales legalmente establecidas para la creación de bases de datos de carácter personal. Así, será necesario que la persona o entidad que vaya a proceder a la creación de tal base de datos, notifique previamente tal circunstancia a la AEPD de acuerdo al art. 26 de la LOPDP. En tal notificación deberá hacerse constar, entre otros: el responsable de la base de datos; su finalidad, publicitaria en este caso; el tipo de datos de carácter personal que contiene; las medidas de seguridad previstas; las cesiones de datos que se prevea realizar; y, en su caso, las transferencias de datos que se prevean a terceros países. Si esta notificación cumple los requisitos exigibles, el Registro General de Protección de Datos procederá a la inscripción de la base de datos; en caso contrario, podrá pedir que se completen los datos que falten o se subsanen. En la legislación venezolana esto no está contemplado.

De igual modo señala Fernando (2005: 106), en la LOPDP se recogen una serie de obligaciones exigibles a los responsables de los ficheros de titularidad privada, derivadas del reconocimiento de los derechos de acceso, rectificación, cancelación y de oposición reconocidos a los ciudadanos, y que deberán ser cumplidas por los responsables de las bases de datos personales con fines publicitarios. En el caso de Venezuela, estas acciones las consagra el constituyente (art. 28) en forma general tanto para bases de datos públicas como privadas, requiriéndose un regulación especial, dado que en el caso particular de las bases de datos personales con fines publicitarios no existe normativa alguna. Sólo en dos categorías jurídicas se contemplan estos principios; por una parte, la Ley de la Función Pública de Estadística (art. 15)[2], contempla estos derechos pero de manera limitada y, es limitada porque

[1] Artículo 38. Los órganos de las distintas ramas del Poder Público, ordenarán los registros y archivos de sus actividades que puedan tener utilidad estadística, creando para ello una base de datos para facilitar, tanto el aprovechamiento de datos administrativos a efectos estadísticos, como la entrega a los interesados de cualesquiera informaciones contenidas en dichos registros y archivos en los términos que establezca la legislación sobre la materia. Asimismo están obligados a recoger y producir datos estadísticos relacionados con el ejercicio de su competencia

[2] **Artículo 15.** Los interesados tendrán derecho al acceso de los datos personales que figuren en las bases de datos estadísticos no amparados por el secreto

sólo se refiere a un sector que además es público, como lo es el sistema de información estadística, donde se manejan datos de naturaleza pública, lo cual resulta lógico por ser una ley sectorial sólo para el caso de datos para bases estadísticas y que no estén bajo la figura del secreto estadístico . Y la otra categoría jurídica es el aún no vigente, porque cuenta con una *vacatio legis* de dos años, se hace referencia al Decreto No. 9.051, cuyo ámbito de aplicación es público también, pues su objeto según su art. 1 es: "El presente Decreto con Rango, Valor y Fuerza de Ley tiene por objeto establecer las bases y principios que regirá el acceso e intercambio electrónico de datos, información y documentos entre los órganos y entes del Estado, con el fin de garantizar la implementación de un estándar de interoperabilidad.". En consecuencia, por su ámbito de aplicación[1] no es posible aplicarla por analogía o extrapolación al ámbito privado o comercial.

4.2. La comunicación de datos a terceros con fines publicitarios

La comunicación de datos está sometida, al igual que su obtención, al principio del consentimiento del titular de los datos. En este sentido, el art. 11 de la LOPDP dispone que, en general, los datos de carácter personal sólo podrán ser comunicados a un tercero con el consentimiento previo

estadístico y a exigir que sean rectificados los datos que les conciernan, al demostrar que son inexactos, incompletos, equívocos o desactualizados.

[1] Están sometidos a la aplicación de las disposiciones del presente Decreto con Rango, Valor y Fuerza de Ley: 1. Los órganos del Poder Público Nacional, Estadal y Municipal. 2. Los institutos públicos nacionales, estadales, distritales y municipales. 3. El Banco Central de Venezuela. 4. Las Universidades públicas nacionales autónomas y experimentales, así como cualquier otra institución del sector universitario de naturaleza pública. 5. Las demás personas de derecho público nacionales, estadales, distritales y municipales. 6. Las sociedades de cualquier naturaleza en las cuales las personas a que se refieren los numerales anteriores tengan una participación en su capital social superior al cincuenta por ciento (50%), las que se constituyan con la participación de aquéllas, o que a través de otro mecanismo jurídico, tenga el control de sus decisiones. 7. Las fundaciones y asociaciones civiles y demás instituciones creadas con fondos públicos, o que sean dirigidas por las personas a que se refieren los numerales anteriores, o en las cuales tales personas designen sus autoridades, o cuando los aportes presupuestarios o contribuciones efectuados en un ejercicio, por una o varias de las personas a que se refieren los numerales anteriores, representen el cincuenta por ciento (50%) o más de su presupuesto.8. Los demás entes de carácter público. (Art. 3 *ejusdem*)

del interesado, que deberá haber sido informado de la finalidad a la que se destinarán tales datos. En el caso de Venezuela la Ley de la Función Pública de Estadística también consagra en la materia lo propio. Art. 21[1] .

Así pues, en España si la cesión de datos va a llevarse a cabo con fines publicitarios, el interesado deberá ser informado expresamente de tal circunstancia. El art. 27 de la LOPDP, obliga al responsable de la base de datos a informar a los afectados, en el momento en que se efectúe la primera cesión de datos, indicando: la finalidad de la base de datos, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

En este sentido, en Venezuela la Ley de Indepabis sólo consagra, por una parte la autorización para ceder información (art. 37)[2] y, por la otra, el derecho a detener tal cesión (art. 38)[3].

Luego de lo argüido, es necesario precisar algunas excepciones y según Fernando (2005: 106), señala que:

> "excepcionalmente, no se requerirá el consentimiento del interesado cuando: 1. La cesión está autorizada en una ley; 2. Se trate de datos recogidos de fuentes accesibles al público; 3. El tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente

---

[1] **Artículo 21.** La obligación de guardar el secreto estadístico nace en el momento en que los datos son obtenidos. Los datos relativos a personas naturales protegidos por el secreto estadístico no pueden ser facilitados para su consulta pública sin que medie consentimiento expreso del afectado, o hasta que haya transcurrido un plazo de veinte años desde la muerte de éste, si su fecha es conocida, o, en otro caso, de treinta años a partir de la fecha de obtención de los datos. Excepcionalmente, transcurridos al menos veinte años desde que los órganos estadísticos obtuvieron la información, podrán ser suministrados datos personales, protegidos por el secreto estadístico a quienes prueben un legítimo interés...

[2] **Artículo 37.** En las negociaciones electrónicas, la proveedora o el proveedor deberán garantizar a las personas la privacidad y la confidencialidad de los datos e información implicada en las transacciones realizadas, de forma tal que la información intercambiada no sea accesible para terceros no autorizados.

[3] **Artículo 38.** En el comercio electrónico la proveedora o el proveedor deberá otorgar a la consumidora o consumidor o la usuaria o usuario, la posibilidad de que pueda escoger, entre la información recolectada, aquella que no podrá ser suministrada a terceras personas, indicar si el suministro de información sobre las personas es parte integrante del modelo de negocios de la proveedora o proveedor, señalar si las personas tendrán la posibilidad de limitar el uso de información personal, y como la podrán limitar.

> la conexión de dicho tratamiento con ficheros de terceros; 4. La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Público o los Jueces o Tribunales , en el ejercicio de las funciones que tiene atribuidas; 5. Se produzca la cesión entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos y; 6. La cesación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad.

Después de lo planteado vale resaltar algunos aspectos:

a) En España la LSSICE contiene varios preceptos que regulan las comunicaciones comerciales electrónicas y que inciden, en particular, en la protección de datos de carácter personal. Pero en todo caso, tales disposiciones deben considerarse complementarias respecto a las establecidas en la LOPDP. En el caso de Venezuela, no hay legislación especial en la materia de protección de datos o habeas data y, aunque existe un marco legal, este es sectorial, ha sido a través de la jurisprudencia vinculante de la Sala Constitucional del TSJ, que se ha logrado la protección de estos datos. Y vale aclarar, que no tiene sentido aplicar analogías o tratar de regular la situación con base a leyes de otros ámbitos, pues el habeas data o autodeterminación informativa es un derecho y una garantía constitucional, que por mandato constitucional exige una legislación propia, entonces hay que tener cuidado de aplicar forzadamente regulaciones a situaciones que tienen particularidades y diferencias, pues si fuese así, con aplicar la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales: Gaceta 34060, estaría resuelto lo referente a la protección de los datos, porque algunos autores consideran la protección de los datos como un amparo especialísimo y, no es así[1].

b) El consentimiento del titular de los datos resulta fundamental para el tratamiento de los mismos por parte del tenedor de la bases de datos o de terceros y, es un principio universalmente aceptado. Sin embargo, se han visto excepciones, pues como se ha indicado no se pretende con la protección de los datos evitar su tratamiento, sino que este tratamiento sea responsable, por lo cual no se trata de introducir nuevas obligaciones para los responsables de las bases de datos en este caso en línea, sino detallar la

[1] Se puede consultar Ortíz, R. (2001). **Habeas Data. Derecho Fundamental y Garantía de Protección de los Derechos de la Personalidad (Derecho a la Información y Libertad de Expresión)**. Editorial Frónesis, S.A. Caracas.

forma en que han de actuar la entidades que operan en línea, para así dar cumplimiento a las obligaciones establecidas.

c) En el caso de España se cuenta con un marco regulador eficiente, esto lo demuestran datos estadísticos de la AEPD de septiembre de 2011[1], mientras que en el caso de Venezuela como parte de la OCDE y de la Red iberoamericana de protección de datos, se está en mora legislativa, por lo cual debe darse cumplimiento a los principios que conforman las medidas de autocontrol (como por ejemplo códigos de ética y principios universales acogidos por las partes en la relación contractual) y a las medidas de heterocontrol (como las Líneas, Leyes Modelos, Directivas o Principios establecidos por Organismos Internacionales) especialmente en el ámbito privado hasta que se tenga un régimen de protección adecuado en el país y en casos de carácter público los establecidos por algunas normas sectoriales.

5. La noción de actividad comercial y la protección de los consumidores en el momento de la Publicidad

Parece entonces indispensable promover una seguridad de los intercambios electrónicos comerciales y crear un marco jurídico transparente y tranquilizante para los usuarios de la red, es por ello que debe existir una política de reconocimiento del valor jurídico de los instrumentos de una transacción en el mundo virtual de Internet. Más aún cuando la mayoría de las empresas han creado su propia página Web, como soporte de comunicación. En ocasiones, esta página Web es sólo una página de información de los productos y servicios que la empresa ofrece, pero en otras puede ser una verdadera publicidad de esos productos y servicios[2]. Si se parte de la noción de publicidad como toda aquella información susceptible de inducir a una persona a hacer una elección sobre un producto o servicio determinado, es difícil en Internet distinguir fácilmente entre publicidad e información.

Según Llobet (1996: 66-67), "se discute si en realidad la publicidad constituye un medio de información del consumidor". En contra se argumenta que la finalidad principal de la publicidad no es informar, sino convencer.

---

[1] Ficheros inscritos en el Registro General de Protección de Datos suman un total de 2.504.844 para el 30-09-2011, entre públicos y privados, sean modificado 6.343 ficheros y sean suprimido 47-549 ficheros para esta fecha entre solicitud de parte y subsanaciones de la Agencia. Ver más detalles En. www. agpd.es/portaleswebAGPD(ficheros_inscritos/estadísticas/common/pdfs/2011/est201109.pdf (Fecha de Consulta 30-10-2011)

[2] Por ejemplo *www.amazon.com, www.telovendo.com, www.mercadolibre.com*

No obstante, no debe olvidarse que muchas veces la publicidad es el único medio de que dispone el consumidor para obtener datos sobre determinado producto o servicio"[1] . Se comparte con el autor que este argumento debe prevalecer sobre el anterior, y en consecuencia considerar a la publicidad como un medio de información del consumidor, si bien con determinadas características que le confieren una singularidad especial.

Señala Ovilla (2003), nuevas formas de publicidad aparecen en Internet. Entre ellas pueden distinguirse: 1) cuando un usuario utiliza los motores de búsqueda para encontrar la información deseada, conocido en inglés como *pull*, y que al momento de recibir los resultados de la búsqueda puede encontrarse "inundado" de publicidad, [2] la cual no le interesa[3]. La búsqueda con la ayuda de portales de clasificación de información vía temas y/o países[4] tampoco esta exenta de la publicidad. El orden de presentación del conjunto no es aleatorio, es posible influenciar a un consumidor por este orden de presentación. 2) cuando el usuario recibe mensajes que no pidió, llamado en inglés *push.*

El usuario de Internet, que desea encontrar ciertos contenidos dentro de la gran cantidad de información que se obtiene vía Internet, debe al mismo tiempo evitar los contenidos ofensivos ilegales y la publicidad no deseada. Es necesario resolver jurídicamente este problema de invasión de la intimidad, tal vez la solución sea la regulación de la industria.[5] Sin embargo, dado el carácter internacional e inmaterial de esta forma de publicidad, su control resulta de difícil aplicación.

"La publicidad por Internet debe de respetar la legislación local y también la legislación de los países hacia los cuales va dirigida. Una publicidad lícita en un país puede que no lo sea en otro", así lo afirma Varille (1997: 5). Así,

---

[1] Caso por ejemplo del cliente de una entidad financiera que solicita disponer de una tarjeta de crédito. La única información que ha recibido sobre la tarjeta ha sido proporcionada por la publicidad que la entidad financiera ha hecho de ella. El solicitante de la tarjeta no conocerá el verdadero alcance de las obligaciones que asume hasta después de haber firmado el documento que contiene las condiciones generales

[2] Es posible el envío de una publicidad que se relacione con el tema o las palabras que se buscan a la ayuda de un motor de búsqueda. Es la cibermercadotecnia.

[3] Y que puede retardar la visualización de la página Web que interesan al usuario. En realidad, el usuario paga de cierta manera el costo de esta publicidad.

[4] Como es el caso de Yahoo.

[5] Por ejemplo, la regulación de la utilización de *cookies*

por ejemplo, se puede mencionar: la publicidad de productos alcohólicos y de cigarros se encuentra prohibida en Francia y, en México está permitida, entonces ¿qué legislación aplicar?

Actualmente existe una serie de recomendaciones, códigos de conducta dirigidos a las empresas y organizaciones para el control del comercio internacional, en lo relativo a actos ilícitos[1]. Por tanto, el anunciante tiene la obligación de identificarse, de informar al usuario las razones de una posible recopilación de datos nominativos, el respeto de la confidencialidad, se le prohíbe utilizar la técnica de *spam*[2], así como debe respetar ciertas disposiciones particulares sobre la publicidad infantil y el respeto de las sensibilidades diversas de la comunidad internacional.

En este sentido, siguiendo a Ovilla (2003:5-6) algunos lineamientos pueden ser:

1. Los anunciantes deben designar al destinatario de la publicidad de una manera expresa, dando una lista de los países a quien esta publicidad va destinada, además de un criterio lingüístico, el idioma y/ o por medio de la utilización de símbolos nacionales, como la bandera del país a quien la publicidad va dirigida.

2. En el caso de que sea un anuncio publicitario que suponga una oferta debe tener las siguientes características: identidad del proveedor, las características especiales del producto, el precio (si tiene los impuestos incluidos o no), y en su caso los gastos de transporte, la forma de pago y las modalidades de entrega o de ejecución de servicios, además de especificar claramente el plazo de la validez de la oferta.

3. Existen ciertos principios para determinar la legislación aplicable: a) Aplicar los Convenios Internacionales (decir cuáles son, aplicar la legis-

[1] Estas reglas materiales internacionales son consecuencias de las Convenciones Internacionales reguladoras del comercio internacional. Existe así una extra comercialidad internacional que tiene por objeto el reconocimiento de una lista de cosas que se encentran fuera del comercio. Por ejemplo La Recomendación de la Cámara de Comercio Internacional sobre la exacción y la corrupción en las transacciones internacionales de 1997; las Recomendaciones de la Directiva del CEE del 14 de junio de 1989 que prohíbe la comercialización de cuerpo humano, Los principios directivos de la OCDE para las empresas multinacionales de 1976.

[2] Se llama *spam*, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina *spamming*. Ver *www.wikipedia.org* (Fecha de Consulta 30-10-2011)

lación del vendedor, aplicar la legislación del comprador); b) Crear normas especificas para Internet; c) Aplicar el sistema de "nombres de dominio", (teniendo en cuenta que habría que tener un control del mismo para que el primer nivel coincida siempre con el territorio del país correspondiente. Así, el lugar de donde partió la oferta (el país donde se halle el servidor) será el criterio a utilizar para aplicar la ley). Por supuesto en lo que corresponde a los dominio .com este criterio no podrá ser aplicado, pero en los otros dominios sí.

4. Actualmente, las únicas soluciones posibles son la autorregulación de las partes involucradas (publicistas, creadores de sitios web, empresarios, consumidores, autoridades). Y la coordinación de los Estados a nivel internacional para crear un mínimo de armonización sobre las prácticas publicitarias que se encuentren prohibidas o reglamentadas. No obstante, existen disposiciones penales referidas a la protección de datos personales, por ejemplo, las ubicadas en el Código Penal suizo y su ley federal de protección de Datos. Señala Javato (2005: 6) que el artículo 178 *novies* del Código penal suizo castiga la sustracción indebida de datos personales. En el caso de Venezuela existe la ley especial contra los delitos informáticos[1], que señala en sus artículos 14, 16 y 20, las sanciones correspondientes en caso de manipulación, sustracción, alteración o supresión de la data.

Finalmente, con base a los principios se recomienda que la deontología este presente como en todo otro soporte publicitario. En consecuencia, la primera regla a aplicar, por las empresas comerciales, es la identificación de carácter publicitario del mensaje[2] . La segunda regla, es relativa a la protección de los datos nominativos de los clientes. Al momento de hacer un pedido, los clientes deben llenar un formulario donde se les pide proporcionar sus datos generales, nombre, dirección, teléfono, dirección de correo electrónico, etc. El cliente debe ser informado que salvo aviso contrario de su parte estos datos pueden ser "vendidos" a otras sociedades o utilizados para enviarle publicidad de la empresa.

---

[1] Gaceta Oficial de la República Bolivariana de Venezuela No. 37.313 Ley especial contra los delitos informáticos, de fecha 30 de octubre de 2001

[2] Principio existente en el Código Internacional de prácticas locales en materia de publicidad de la Cámara Internacional de Comercio.

6. Principios para la protección de datos de carácter personal en el medio electrónico

Al hacer un recuento de las actividades que realiza un consumidor para llevar a cabo una transacción de compra y venta electrónica, y considerando lo expuesto anteriormente, se puede identificar que en una compra venta por Internet o cualquier otro medio electrónico, para proteger la privacidad del consumidor, siguiendo a Chen (2010: 125-126) se debe cumplir lo siguiente:

1. Informar al consumidor, si el sitio que accede está grabando "cookies" en su computador, y las consecuencias de ello.
2. El consumidor debe ser responsable de informarse para fijar el nivel de seguridad adecuado a sus intereses.
3. Informar al consumidor: a) 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 y b) sobre el nivel de protección que tendrán sus datos y que éstos no serán cedidos, vendidos o transferidos a terceros sin su consentimiento.
4. 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 tal recolección. Consultar al consumidor, si desea que se le envíe publicidad a su dirección de correo electrónico o cuando se encuentre navegando por Internet.
5. Informar al consumidor sobre sus derechos sobre los datos, si puede consultarlos, rectificarlos, oponerse a su procesamiento, o acceder a ellos en cualquier momento.
6. Los datos que se recolecten deben ser exactos, pertinentes, adecuados, no excesivos y utilizados conforme al fin establecido (para 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)
7. Prohibir que se interconecten archivos para procesar datos de un consumidor para obtener perfiles de sus actividades, sin su consentimiento expreso.
8. Prohibir la recolección de datos sensibles que puedan después utilizarse para negar una venta o un servicio al consumidor, o tratarlo de manera diferente.

9. 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 puedan cambiar su valoración inicial
10. 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.
11. El Estado debe informar y educar a las personas para que puedan establecer relaciones de consumo responsable (tome sus propias medidas de seguridad).

En definitiva, hay unos *Principios Básicos:* 1. Informar al consumidor y obtener su consentimiento. 2. Limitación de objetivos, es decir, los datos deben utilizarse con una finalidad específica. 3. Proporcionalidad y calidad de los datos. 4. Transparencia. 5. Seguridad. 6. Derecho de acceso, rectificación y oposición. 7. Restricciones respecto a ulteriores transferencias a países terceros. Y como *Principios Adicionales* serían: 1. Tratamiento de Datos sensibles. 2. *Marketing* directo. 3. Mecanismos de procedimiento/aplicación, es decir, un sistema adecuado debe ofrecer tanto un nivel satisfactorio de cumplimiento de las normas como un apoyo y asistencia a los interesados en el ejercicio de sus derechos (Álvarez, 2005)

Conclusiones

El consumidor en el comercio electrónico, tienen por una parte el derecho fundamental de información y, por otra a que la información que ofrece a través de estos sitios web, sea objeto de protección, especialmente aquellos datos de carácter personal, aspecto que medianamente aborda la legislación de Venezuela y, que se ve en la necesidad de complementar con sentencias de la Sala Constitucional, ante la ausencia de la ley especial a la cual se refiere el constituyente en el art. 28.

El consumidor o usuario puede ser víctima de irrespeto a su dignidad como persona o víctima de fraude a su patrimonio y, uno de los escenarios donde se corre un riesgo alto es en la red de redes y, si bien existe en Venezuela una moderada legislación que protege los datos en la esfera de algunos sectores de gobierno o públicos, no ocurre lo mismo en el ámbito del comercio electrónico, como se ha entendido en sentido amplio. Por ello, desde el momento mismo de la publicidad, el consumidor debe tener

garantía de la protección de los datos que ofrece o suministra en línea, a fin de profundizar en la descripción del producto o servicio o para en lo sucesivo recibir información publicitaria sobre otros bienes y servicios de su posible interés.

Se puede permitir el envío de comunicaciones comerciales a aquellos usuarios que: a) previamente lo hubieran autorizado, b) lo hubieran solicitado de forma expresa o, c) cuando con ellos exista una relación contractual previa, en cuyo caso, se podrá enviar publicidad sobre productos o servicios similares a los contratados por el cliente.

La primera regla a aplicar, por las empresas comerciales, es la identificación de carácter publicitario del mensaje. La segunda regla, es relativa a la protección de los datos nominativos de los clientes. Al momento de hacer un pedido, los clientes deben llenar un formulario donde se les pide proporcionar sus datos generales, nombre, dirección, teléfono, dirección de correo electrónico, etc. El cliente debe ser informado que salvo aviso contrario de su parte estos datos pueden ser "vendidos" a otras sociedades o utilizados para enviarle publicidad de la empresa.

Referencias Bibliográficas

ADAPTA SOLUCIONES CONSULTORA EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: En *http://www.adaptasoluciones.com* Fecha de consulta 08 de noviembre de 2011

ÁLVAREZ, Cecilia. 2005. "Las transferencias internacionales de datos personales y el nivel equiparable o adecuado de protección". En **Actualidad Jurídica, No. 12.** Artículos Uría Menéndez. España. p 19-30.

ÁLVAREZ, Javier. 2006. Publicidad, Protección de Datos y comunicaciones Comerciales Electrónicas. En: http:// *www.readpyme.net* Fecha de Consulta 25 de enero de 2012.

CHEN, Susan. 2010. "Privacidad y protección de datos: Un análisis de legislación comparada". En: **Diálogos, Revista Electrónica de Historia,** Vol. 11. No. 1. Febrero/Agosto 2010. Costa Rica. p. 111-152.

CONSTITUCIÓN DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA. G.O. 36.860 del 30 de diciembre de 1999

DECRETO CON FUERZA Y RANGO DE LEY DE LA FUNCIÓN PÚBLICA DE ESTADÍSTICA DE VENEZUELA del 09-11-2001

DECRETO CON FUERZA Y RANGO DE LEY PARA LA DEFENSA DE LAS PERSONAS EN EL ACCESO A LOS BIENES Y SERVICIOS DE VENEZUELA del 01-02-2010

DECRETO N° 9.051 (GACETA OFICIAL N° 39.945 del 15 -06- 2012)

DICCIONARIO DE INFORMÁTICA. En. *www.alegsa.com.ar* Fecha de consulta 01-10-2012.

DIRECTIVA ESPAÑOLA 24/2006/CE

FERNANDO, María del Rosario. 2005. "La protección de datos personales" En **Revista de Derecho Informático**. No. 7. Chile. p. 97-109

HERNÁNDEZ, Javier. 2005. Algunos aspectos Legales. En: **Boletines Electrónicos** En http:// *www.proteccionlegal.com* Fecha de consulta 12 de diciembre de 2011.

HUET, J y MAISL, H. 1988. ***Datenschutzgesetz in der ab* 1 de marzo de 1988 *geltenden Fassung.*** Viena.

JAVATO, Antonio. 2005. "La tutela penal del consumidor en el comercio electrónico en el derecho suizo". En **Revista Electrónica de Ciencia Penal y Criminología, Reflexiones** No. 07-r2, p.r2:1-r2:6

LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE ESPAÑA 15/1999 de 13 de diciembre DE 1999.

LEY 25/2007 DE CONSERVACIÓN DE DATOS DE ESPAÑA de fecha 18-10-2007

LEY DE REGISTRO DE ANTECEDENTES PENALES DE VENEZUELA del 31-08-1979

LEY ESPECIAL CONTRA DELITOS INFORMÁTICOS Gaceta Oficial de la República Bolivariana de Venezuela No. 37.313 del 30-10-2001

LEY ORGÁNICA PARA LA PROTECCIÓN DEL NIÑO, NIÑA Y ADOLESCENTE DE VENEZUELA del 07-12-2007.

LEY PARA LA DEFENSA DE LAS PERSONAS EN EL ACCESO A LOS BIENES Y SERVICIOS, Gaceta Oficial de La República Bolivariana de Venezuela Número 39.358, Caracas Lunes 1 de Febrero de 2010

LEY SOBRE PROTECCIÓN A LA PRIVACIDAD DE LAS COMUNICACIONES DE VENEZUELA del 16-12-1991

LLOBET, Josep. 1996. **El deber de información en la formación de los contratos**. Marcial Pons, Ediciones Jurídicas y Sociales, S.A. Madrid.

LÓPEZ, Leticia. 2008. "La conservación de los datos por los operadores de servicios de comunicaciones electrónicas. Análisis de la Ley 25/2007, de 18 de octubre , sobre conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación". En **Actualidad Jurídica, Foro de Actualidad.** No. 19**.** Uría Menéndez. España. p. 71-77

LORENZINI, Jaime. 2000. **Derecho de Información de consumidores**. Vlex, Chile.

LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN (LSSICE) , Ley 34/2002 de fecha 11 de julio de 2002

MARTÍNEZ, Apolonia. 1998. **Comercio electrónico, firma digital y autoridades de certificación.** Madrid. Civitas.

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO *www.ocde.org*

ORTIZ, Rafael. 2001. **Habeas Data. Derecho Fundamental y Garantía de Protección de los Derechos de la Personalidad (Derecho a la Información y Libertad de Expresión)**. Editorial Frónesis, S.A. Caracas.

OVILLA, Rocio. 2003. "¿Quién le teme al Comercio Electrónico? Protección del consumidor en el ámbito digital: el caso de México" En: ***DEA Informatique et Droit, IRETIJ.*** p. 1-14

PANIZA, Antonia. 2006. "E- Consumidores: Aspectos Problemáticos en la normativa española". En: **Revista Chilena de Derecho Informático.** No. 8. Chile. p 15-28.

PÉREZ, Alejandro. 2010. **Crawlers, programas araña en email marketing. LOPD, LSSICE y AEPD**. En: *www.teenvio.com.es* (Fecha de Consulta 1-10-2012)

PROYECTOS: LEY DE PROTECCIÓN DE DATOS Y HABEAS DATA EN VENEZUELA 2004 y PROYECTO DE TECNOLOGÍA DE LA INFORMACIÓN 2004

RICO, Mariliana. 2005. **Comercio Electrónico Internet y Derecho.** 2da edición. Editorial LEGIS, SA. Colombia.

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS. En *http://www.redipd.org.* Fecha de consulta 16 de octubre de 2011.

RODRÍGUEZ, Gladys. 2012. Riesgos del consumidor electrónico en las prácticas publicitarias. En: **Revista de Derecho.** Universidad del Norte. No. 37. Colombia. P 254-282.

TRIBUNAL SUPREMO DE JUSTICIA. SENTENCIA N°. 332, Expediente No: 00-1797. Caso Insaca. Sala Constitucional del TSJ de fecha 14 de marzo de 2001. Ponencia Jesús E. Cabrera

TRIBUNAL SUPREMO DE JUSTICIA. SENTENCIA N° 940. Caso: Asdrúbal Celestino Sevilla. Sala Constitucional del TSJ de fecha 21 de mayo de 2007. Ponencia Carmen Zuleta de Merchán. En: *http://www.tsj.gov.ve/decisiones/scon/mayo/940-210507-03-2352.htm*. Fecha de consulta: 29-09-2012.

TRIBUNAL SUPREMO DE JUSTICIA, SENTENCIA N° 1318. Caso: Nulidad de la Decreto N° 1.526 con Fuerza de Ley de Reforma de la Ley General de Bancos y otras Instituciones Financieras. Sala Constitucional del TSJ de fecha 12 de junio de

2012. Ponencia Luisa Estella Morales. En: *http://www.tsj.gov.ve/decisiones/scon/Agosto/1318-4811-2011-04-2395.html.* Fecha de consulta: 29-09-2012.

VARILLE, Nathalie. 1997. ***Publicité sur Internet, Droit et Déontologie,*** *Gazette du Palais,* 22de noviembre de 1997, Paris, p. 4-10.