La importancia de la protección de datos de carácter personal en las relaciones comerciales.

Aproximación al Derecho venezolano

Emercio José Aponte Núñez

Sumario: *I. Premisa.- 2. Definición de la protección de datos personales-. 3. ¿Qué supone la protección de datos personales?.- 4. ¿Pueden las empresas estar sujetas a la protección de datos?- 5. Principios sobre los cuales descansa la protección de datos.- 6. Derechos que comprende la protección de datos.- 7. Importancia y utilidad de los datos personales en la actividad comercial.- 8. Situación del ordenamiento jurídico venezolano. 9. Los códigos de conducta.*

I. PREMISA

En el mundo de hoy los avances tecnológicos han permitido a los hombres salvar el espacio, y el desarrollo de la informática ha facilitado la posibilidad de almacenar gran cantidad de datos personales, referidos, entre otros, a la infancia, la vida familiar, académica y profesional, los gustos, lugar de habitación, uso de tarjetas de crédito, creencias religiosas, afiliaciones políticas, etc.

"Por primera vez desde la invención de la escritura el hombre (...) podrá servirse de la considerable cantidad de documentación (impresa) que existe actualmente en el mundo [...] de una manera tan ágil, directa y sencilla, como si estuviera conversando con su vecino. Esto es lo que la moderna tecnología de los ordenadores aporta"[1]. Lo anterior hace posible alcanzar un conocimiento integral de actitudes, capacidades, tendencias, pautas de comportamiento que se circunscriben a una esfera muy íntima de las personas. Pero además, ese conocimiento se constituye en una herramienta invaluable que permite delinear el perfil comercial de las personas, y determinar apreciaciones positivas o negativas de las mismas.

1 A. La Roche, *La protección del comercio electrónico,* en *La Nueva Ley de Protección al Consumidor y al Usuario. Análisis crítico*, Maracaibo, 2004, 76.

Esa situación ha generado una serie de regulaciones protectoras de esos datos de carácter personal que, conscientes de la importancia de la informática para la actividad comercial, buscan un equilibrio entre la protección de los datos mismos y el uso del medio tecnológico.

Es claro que para abordar este tema bajo su verdadera dimensión e importancia se necesitan más que unas breves líneas, lo que aquí se busca, mediante las reflexiones reflejadas en este trabajo, es ir creando conciencia de la necesidad de proteger los datos de carácter personal, tanto en los empresarios, sea que estemos hablando de personas jurídicas o de personas naturales o físicas, como en los particulares, los primeros en calidad de responsables del tratamiento de datos de carácter personal y los segundos en su condición de titulares de esos datos.

Para ello, se utilizarán esencialmente, como base de este trabajo, las directrices para la regulación de los archivos de datos personales informatizados de las Naciones Unidas, la Directiva 95/46/CE, la Ley Orgánica de Protección de Datos de Carácter Personal de España, la Declaración de Cartagena de Indias de la Red Iberoamericana de Protección de Datos, la Constitución de la República Bolivariana de Venezuela, el anteproyecto de Ley de Protección de Datos y Habeas Data para Venezuela, la Ley de Protección al Consumidor y al Usuario venezolana, la Ley de Igualdad de Oportunidades para la Mujer de Venezuela, la Ley de Registro de Antecedentes Penales venezolana y la Ley Especial contra los Delitos Informáticos de Venezuela.

2. DEFINICIÓN DE LA PROTECCIÓN DE DATOS PERSONALES

La protección de datos de carácter personal se puede definir como "el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad"[2].

De esta definición es conveniente y necesario, para una mejor comprensión del tema tratado en el presente trabajo, tener claro el significado de los siguientes términos: a. Ciudadano; b. Datos personales (con especial referencia al correo electrónico); c. Tercero; y, d. Tratamiento.

a. Ciudadano: es toda persona natural o física titular de los datos de carácter personal, susceptibles de tratamiento automatizado, que lo identifican o lo hacen identificable. Por lo que las personas jurídicas no son sujetos de esta protección, tal como será analizado más adelante.

b. Datos de carácter personal: es toda información perteneciente a una persona natural o física que la identifica o la hace inidentificable y es susceptible

2 *Anuario del Derecho de las Tecnologías de la Información y las Comunicaciones (TIC)*, M. DAVARA RODRÍGUEZ (Coord.). España, 2004, 3.

de tratamiento automatizado. El alcance de esta definición implica que todo tratamiento de datos de carácter personal realizado en forma disociada de la persona de su titular no es objeto de las normas reguladoras en esta materia, ya que al no poder asociar la información objeto de tratamiento con la persona titular de los mismos no existe la posibilidad de afectar su intimidad.

En relación con el correo electrónico surge la pregunta: ¿podrá ser considerado como un dato de carácter personal? La duda surge en virtud de la forma como está conformada la dirección electrónica, la cual comprende dos parámetros: el *login*, seleccionado por el usuario de la dirección, y el nombre de dominio, que identifica a la empresa prestadora del servicio de correo electrónico, precedido del símbolo arroba.

En este sentido la Agencia Española de Protección de Datos en su Memoria de 2000, y dando respuesta a la interrogante antes planteada, expresó: "En el supuesto de direcciones electrónicas la información está constituida por un conjunto de signos que cuando permiten la vinculación directa o indirecta con una persona física lo convierte en un dato de carácter personal"[3]. De esta forma, el correo electrónico sólo tendrá el carácter antes expresado cuando se logre, en virtud del tratamiento, la vinculación con la persona titular del mismo, es decir cuando se pueda establecer la relación entre el correo electrónico y la identidad de su titular.

c. Tercero: es toda persona física o jurídica que, sólo o conjuntamente con otras, se encarga de tratar los datos de carácter personal de personas físicas. En este caso hablamos tanto de personas naturales como jurídicas, a diferencia del significado de la expresión ciudadanos, que únicamente comprende las personas naturales o físicas titulares de los datos personales.

d. Tratamiento: son las operaciones, automatizadas o manuales, mediante las cuales se recogen, graban, conservan, modifican, elaboran, bloquean, cancelan e incluso se ceden o transfieren datos personales.

Para la Red Iberoamericana de Protección de Datos[4] el tratamiento es "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recolección, registro,

3 Memoria Anual de 2002 de la Agencia de Protección de Datos, *CD Agencia de Protección de Datos 2003*.

4 La Red Iberoamericana de Protección de Datos nace en junio de 2003, producto de los encuentros iberoamericanos celebrados anualmente, promovidos por la Agencia Española de Protección de Datos. La Red se crea como un foro permanente cuyo objetivo es potenciar las iniciativas de intercambio de experiencias entre los países iberoamericanos, y otorga un papel esencial a la difusión y colaboración en esta materia, con el objeto de lograr un tratamiento común a los problemas que se vayan presentando, dando soluciones armonizadas. Son miembros de esta Red: Argentina, Brasil, Chile, Colombia, Costa Rica, El Salvador, España, Guatemala, México, Nicaragua, Perú, Portugal y Uruguay. La presidencia de la Red la ostenta en la actualidad el Director de la Agencia Española de Protección de Datos.

organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción"[5].

Es decir, los datos tienen que ser susceptibles de ser tratados de forma automatizada, lo que implica que no sólo aquellos que lleven registros o ficheros bajo esa modalidad deben respetar la normativa protectora, sino también aquellos que lo hagan manualmente, siempre y cuando, en este último caso, exista la posibilidad de automatizar ese proceso.

3. ¿QUÉ SUPONE LA PROTECCIÓN DE DATOS PERSONALES?

La protección de datos personales busca garantizar la privacidad de las personas, el resguardo o protección de su intimidad; lo cual supone, fundamentalmente, la posibilidad real de controlar el uso y la finalidad para la cual se destina la información relativa a los datos personales de cada individuo, y la facultad de oponerse a su utilización, de manera tal de impedir que esa información sirva a propósitos no aceptados por su titular.

Este derecho, en algunos ordenamientos jurídicos como el español y el venezolano, ha adquirido una naturaleza jurídica propia y rango de derecho fundamental distinto al propio derecho a la intimidad, llamado por el Tribunal Constitucional español como libertad informática (*habeas data*).

Incluso, este carácter de derecho fundamental también está reconocido por la Unión Europea, al haberlo consagrado en el Tratado por el que se establece da una Constitución[6]. De igual forma, es conveniente tener presente que los jefes de Estado y de Gobierno de los países iberoamericanos, en la Declaración final de la XIII Cumbre celebrada en Bolivia en el año 2003, expresaron en su punto 45" que la protección de datos personales es un derecho fundamental de las personas".

En definitiva, "el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado"[7].

4. ¿PUEDEN LAS EMPRESAS ESTAR SUJETAS A LA PROTECCIÓN DE DATOS?

Antes de responder la interrogante planteada, es conveniente precisar que el término "empresa" abarca, en el presente caso, tanto a la persona jurídica como a

5 Declaración de Cartagena de Indias, III Encuentro Iberoamericano de Protección de Datos, 25-28 de mayo de 2004.

6 Esta consagración se encuentra plasmada en los artículos I-51 y II-68.

7 J. APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, 2002, 28.

la persona natural o física dedicada a la actividad de carácter comercial, es decir se utiliza este término en un sentido económico más que jurídico.

Hecha la aclaración, se puede afirmar, como ya se hizo anteriormente, que el sujeto de protección es toda persona física titular de los datos que son objeto de tratamiento. Por lo tanto, las personas jurídicas están excluidas de está protección, sin perjuicio de las acciones que puedan ejercer por ante los tribunales competentes, para hacer valer la responsabilidad por daños y perjuicios ocasionados por el uso indebido de los datos o informaciones relacionados con ellas, pero no como violación de su intimidad y del derecho a la protección de datos, sino como consecuencia de un hecho ilícito o del incumplimiento de un contrato.

El problema se plantea cuando hablamos del empresario individual e incluso del profesional. En este caso, la conclusión a que se ha llegado es que estos no se encuentran amparados por el ordenamiento regulador de la protección de datos, ya que su esfera de actividades trasciende la intimidad y la familia.

En ese orden de ideas, la Agencia de Protección de Datos española fundamenta la inaplicabilidad de esta protección a las empresas, tanto a aquellas constituidas en personas jurídicas como al empresario individual, en que "si la protección de los datos personales se refiere a la intimidad personal y familiar, no puede entenderse que las empresas gocen de la citada intimidad. Por tanto, no puede ser aplicada a la empresa la protección, ni siquiera cuando se ejerza directamente por una persona física, puesto que el ámbito personal que se protege debe entenderse distinto del profesional, ya que las normas de protección, la Directiva europea y la Ley española, delimitan la protección a la intimidad respecto de las personas y la familia, conceptos que se refieren a un espacio limitado de donde se excluye la actividad empresarial, que siempre es exteriorizada"[8].

No obstante, los datos del empresario individual y los profesionales, cuando no sea posible diferenciar su actividad mercantil o profesional de su propia esfera de actividad individual, estarán sujetos a protección.

5. PRINCIPIOS SOBRE LOS CUALES DESCANSA LA PROTECCIÓN DE DATOS

Algunos principios sirven de fundamento o base para la protección de datos personales, principios que aportan las garantías mínimas que deben consagrar las distintas legislaciones nacionales. Dentro de estos principios podemos mencionar: a. Consentimiento del titular de los datos; b. Calidad de los datos; c. Información

8 Resolución de la Agencia Española de Protección de Datos R/00202/1998 del 28 de julio de 1998, dictada en el PS/00025/1998. No obstante, es importante tener presente que aunque en la mayoría de las legislaciones las personas ideales o jurídicas no se encuentran amparadas por esta normativa, en otras, como la Ley de Protección de Datos Argentina, sí lo están.

en la recolección de los datos; d. Cesión o comunicación de datos; e. Principio de no discriminación.

a. Consentimiento del titular de los datos: este principio significa que es el titular de los datos la única persona capaz de decidir cuándo, cómo, dónde y quién trata los mismos. Es decir, se requiere un consentimiento de la persona cuyos datos van a ser tratados.

En el Tratado por el que se establece una Constitución para Europa se puede leer: Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Estos datos se tratarán [...] sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento previsto por la ley"[9].

Este consentimiento puede ser expreso o tácito. Cuando es expreso se exige que el titular declare de forma clara e inequívoca su aceptación al tratamiento o cesión de sus datos; lo cual puede hacerse de forma verbal o escrita. Y, el consentimiento tácito proviene, más que de una expresión de voluntad, de una forma de comportamiento que implícitamente demuestra la aceptación, como por ejemplo: su falta de actuación, su silencio. No obstante, este principio cuenta con las siguientes excepciones:

- Cuando se recojan los datos para el ejercicio de las funciones propias de la Administración Pública. En este caso la limitación a esta excepción radica en las mismas competencias y funciones de la Administración Pública, ya que sólo será aplicable la no necesidad del consentimiento cuando el acto se realice dentro de esas facultades; de lo contrario será necesario contar con el consentimiento del titular de los datos personales.

- Cuando se refieran a la parte de un contrato o precontrato y sean necesarios para su mantenimiento o cumplimiento. En relación con está excepción, se puede inferir que el titular de los datos al momento de dar su consentimiento para la celebración del contrato lo está haciendo para el tratamiento de sus datos en la medida en que sea necesario para dar cumplimiento a la finalidad contractual.

- Para proteger el interés vital del interesado.

- Cuando los datos procedan de una fuente pública. Esta excepción implica que se exceptúa el cumplimiento del requisito del consentimiento del titular de los datos que figuren en una fuente pública, mas no excluye la aplicación de la normatividad reguladora de la protección de datos personales en relación con el resto de los principios y derechos propios de esta materia, que deben ser cumplidos por el responsable del tratamiento de los datos.

b. Calidad de datos: "Este principio se concreta en la necesidad de que los datos objeto de tratamiento sean pertinentes, adecuados y no excesivos en relación con las finalidades determinadas, expresadas y autorizadas para las que se hubieran recabado"[10]; además implica la obligación de mantenerlos actualizados, pero

9 Tratado por el que se establece una Constitución para Europa, artículo II-68.

10 DAVARA RODRÍGUEZ, Ob. cit., 4.

ello sólo por el tiempo necesario para cumplir con la finalidad o finalidades que motivaron su registro.

En ese sentido, "las personas responsables de la compilación de archivos, o aquellas responsables de mantenerlos, tienen la obligación de llevar a cabo comprobaciones periódicas acerca de la exactitud y pertinencia de los datos registrados y garantizar que los mismos se mantengan de la forma más completa posible, con el fin de evitar errores de omisión, así como de actualizarlos periódicamente"[11], usándolos, pues, únicamente para el fin por el cual fueron obtenidos y sólo por el tiempo necesario para la consecución del mismo.

c. Información en la recolección de datos: este principio conlleva la obligación por parte de la persona responsable del registro o fichero de informar al titular de los datos personales, previamente a su tratamiento, sobre la existencia del mismo, de la finalidad del tratamiento, de los destinatarios de la información, de la potestad que tiene de abstenerse de responder a las interrogantes formuladas y, además, del derecho de acceso, rectificación y cancelación.

En definitiva, asegura que la información relativa a las personas no se haga por medios desleales, ni para finalidades distintas a las informadas.

d. La cesión o comunicación de datos: garantiza que la cesión de los datos personales se debe hacer previo consentimiento del titular de los mismos, y sólo para dar cumplimiento a los fines directamente relacionados con las funciones tanto del cedente como del cesionario.

e. Principio de no discriminación: mediante éste se prohíbe la recolección de datos que puedan dar origen a una discriminación arbitraria, referida a toda información sobre raza, color, vida sexual, religión, afiliación política o cualquier otra creencia.

6. DERECHOS QUE COMPRENDE LA PROTECCIÓN DE DATOS

Los derechos que comprende la protección de datos personales son la concreción individual de los principios enunciados anteriormente, y generan correlativamente obligaciones o deberes para los responsables del tratamiento de los datos personales.

Es indudable que el titular de los datos tiene el derecho de conocer todo lo relacionado con el tratamiento de sus datos personales, que es lo que la doctrina ha denominado el *derecho a la autodeterminación informativa*.

Ahora bien, desde la óptica de las obligaciones que se derivan para el responsable del tratamiento de los datos, los particulares tienen *derecho de acceso,* de *rectificación* y de *cancelación*.

11 Directrices para la regulación de los archivos de datos personales informatizados, adoptadas mediante Resolución 45/95 de a Asamblea General de las Naciones Unidas el 14 de diciembre de 1990.

– *Derecho de acceso*: este derecho supone la facultad que tiene el titular de los datos de dirigir al responsable del tratamiento una solicitud de información en relación con esa actividad.

La finalidad de esta facultad es garantizar al titular de los datos el conocer "qué información está siendo objeto de tratamiento y, con ello, la que puede llegar a obtenerse de los datos"[12].

Su ejercicio, al igual que el derecho de rectificación y cancelación, es de carácter personalísimo, en el sentido de que sólo el titular de los datos puede ejercerlo frente al responsable del tratamiento. No obstante, nada impide que el mismo sea ejercido por un apoderado con mandato especial, donde conste de forma precisa y expresa esta facultad, ya que en ese caso el apoderado estaría obrando por cuenta y en representación del titular.

"Cualquiera que ofrezca prueba de su identidad tiene derecho a saber si está siendo procesada información que le concierna y a obtenerla de forma inteligible, sin costes o retrasos indebidos"[13]. La manera de hacer uso de este derecho es mediante una declaración de voluntad expresa, clara e inequívoca en ese sentido.

– *Derecho de rectificación*: consiste en la posibilidad que tiene el titular de los datos de exigir al responsable del tratamiento que cumpla con el principio de calidad, corrigiendo los errores o subsanando las informaciones incompletas, y permitiendo que el tratamiento sea reflejo cierto y fidedigno de la realidad.

Al igual que el derecho de acceso y el de cancelación, este derecho es de carácter personalísimo. No existiendo, en principio, impedimento alguno para ejercerlo mediante apoderado con mandato especial para ello, donde conste de forma expresa y clara esta facultad.

Se debe hacer valer mediante solicitud, que, al igual que para el derecho de acceso, tiene que ser expresa, inequívoca y clara, pero además debe precisar sobre qué datos recae la rectificación solicitada.

En relación con este derecho, el Tratado por el que se establece una Constitución para Europa dispone: "Toda persona tiene derecho a obtener su rectificación"[14].

– *Derecho de cancelación*: es la facultad o potestad que tiene el titular de los datos a que los mismos se excluyan del tratamiento, ya sea porque son errados, o por no tener interés en que sean tratados.

Este derecho se puede ejercer sobre la totalidad de los datos sujetos a tratamiento o únicamente en lo referente a alguno de ellos en forma específica. En definitiva, es una facultad unilateral que tiene la persona frente al responsable del tratamiento,

12 APARICIO SALOM, Ob. cit., 153.

13 Directrices para la regulación de los archivos de datos personales informatizados, adoptadas mediante Resolución 45/95 de a Asamblea General de las Naciones Unidas el 14 de diciembre de 1990.

14 Tratado por el que se establece una Constitución para Europa, artículo II-68.

dejando a salvo las causas que justifiquen el mantenimiento del tratamiento por mandato de la ley. Por ejemplo: en aquellos casos donde sea necesario para el cumplimiento y culminación de una relación contractual.

7. IMPORTANCIA Y UTILIDAD DE LOS DATOS PERSONALES EN LA ACTIVIDAD COMERCIAL

La importancia y utilidad del manejo de los datos personales se ve reflejada en lo que se conoce como el *Data Warehouse y el Data Mining*, que permiten satisfacer los requerimientos de información interna de la empresa para una mejor gestión, convirtiendo los datos personales en una herramienta competitiva por hacerlos disponibles a los empleados para el análisis y la toma de decisiones.

"El *Data Warehouse* es un criterio de almacenamiento y manejo de grandes volúmenes de información corporativa donde se integran todos los elementos para mejorar la toma de decisiones Consiste básicamente en aprovechar -utilizando la técnica del *Data Mining*– los datos recogidos de la actividad de la empresa, para tareas de marketing, prospección, detección de problemas, etc., permitiendo entre otras cosas, comerciar de una forma más focalizada y mucho más productiva"[15].

El *Data Mining* es la herramienta que permite extraer de los datos personales toda la información oculta. Se trata de pasar de los simples datos a la obtención del conocimiento de los mismos. Permite "establecer interrelaciones entre esas enormes cantidades de registros diarios, organizándolos en una forma lógica, y así deducir datos que no existían previamente en la base de datos, extraer y analizar perfiles [y descubrir] patrones y tendencias de comportamiento ocultas del pasado que puedan ser útiles para predecir comportamientos futuros"[16].

Pues bien, mediante esos mecanismos se pueden establecer perfiles y hábitos de los consumidores, con la finalidad de obtener un mayor provecho de la publicidad, pero también permite conocer sus debilidades y valerse de esa información para explotarlos.

Razón por la cual dicho tratamiento, vital para ser competitivo y exitoso en la actividad comercial, está sujeto al sistema de protección de datos personales. De esa forma, adquiere gran relevancia para las sociedades mercantiles el hecho de cumplir con la normativa jurídica reguladora de la materia.

Por supuesto, esta importancia no se agota simplemente con el valor que tiene el tratamiento de datos personales internamente en la organización de una empresa, sino que se refleja en el llamado comercio electrónico, entendiendo por éste:

"El vasto conjunto de actividades con finalidad mercantil que se desarrolla mediante el uso de sistemas de procesamiento de datos y de comunicaciones sin

15 Ortíz-Ortíz, *Habeas data. Derecho fundamental y garantía de protección de los derechos de la personalidad (Derecho a la información y libertad de expresión)*, Caracas, 12.

16 Ibíd., 43.

que exista un contacto físico directo entre quien oferta un bien o un servicio y quien lo demanda la denominación cubre no solamente actos comerciales directos, como la compraventa o alquiler, sino también acciones preparatorias o conexas como la publicidad o mercadeo"[17]. Actividad que también es objeto de regulación en resguardo del derecho de protección de datos personales.

Otro aspecto importante en relación con los datos personales y el comercio se encuentra en la posibilidad de tener que realizar, en virtud de la actividad propia de un sociedad mercantil, transferencias internacionales de los datos personales tratados por ella, ya sea a una empresa del mismo grupo o a una tercera sociedad, lo cual implica y requiere la protección de los datos personales de los titulares, en el sentido de tener la garantía de que esa otra empresa del grupo o ajena al mismo se encuentra en un país donde existe una normativa jurídica que asegura los derechos en esta materia.

"La transferencia internacional de datos debe estar sometida a un régimen de garantías para impedir que los principios que rigen el derecho fundamental a la protección de datos se vean vulnerados por el mero traslado de dichos datos a otro país"[18].

De hecho, la normativa de la Unión Europea y de España prohíben, en principio, las transferencias internacionales de datos personales salvo que se compruebe previamente que en el lugar de destino se ofrece una protección semejante a la otorgada en la Unión Europea[19]. Por ello, es importante para los Estados adecuar su ordenamiento jurídico, de tal forma de alcanzar un grado de protección de los datos personales que permitan su reconocimiento como lugar seguro, ya que de esa forma se facilita el intercambio comercial y el desarrollo del comercio electrónico y de los servicios de la Sociedad de la Información.

Por último, la protección de datos también se ve reflejada en relación con la posibilidad de establecer registros de información crediticia o registros de solvencia, que permitan, a las sociedades mercantiles inscritas en los mismos, obtener una información o perfil del individuo, con la finalidad de valorar su capacidad patrimonial y comportamiento crediticio.

En este sentido la Red Iberoamericana de Protección de Datos ha afirmado que "el tratamiento leal, lícito, transparente y ético de datos personales constituye una garantía de la persona que debe ser respetada en la búsqueda de objetivos como velar por la estabilidad del sistema financiero y facilitar el acceso al crédito. La

17 Ibíd., p. 56.

18 Declaración de Cartagena de Indias, III Encuentro Iberoamericano de Protección de Datos, 25-28 de mayo de 2004.

19 Es oportuno aclarar que cuando un Estado se considera inseguro en relación con la protección de datos de carácter personal, existe la posibilidad de lograr la transferencia internacional mediante la inclusión de cláusulas contractuales tipo aprobadas por la Comisión Europea, que permiten establecer las garantías necesarias que suplan la inexistencia de una normativa adecuada en esta materia.

obtención y uso de información personal para mitigar y administrar los riesgos que implica el otorgamiento de crédito debe ir acompañada del respeto de los derechos de las personas en cuanto al tratamiento de sus datos personales. Una protección efectiva de datos financieros propicia que las personas estén más dispuestas a apoyar el flujo de su información"[20].

Así, estos registros o ficheros de morosos deben cumplir con ciertos requisitos, por ejemplo: cuando el pago recaiga sobre varias personas y se trate de obligaciones solidarias, es decir, se refiera a obligaciones cuyo pago pueda ser exigido en su totalidad a cualquiera de los obligados, se debe haber requerido el pago a todos los deudores para poder incluirlos en el registro de morosos; cuando el pago recaiga sobre varias personas y se trate de obligaciones mancomunadas, es decir, obligaciones donde cada uno de los deudores responde por una parte del total adeudado, se incluirá en el registro a todo aquel a quien se haya requerido el pago de la parte correspondiente, y únicamente por el monto obligado a pagar; sólo se puede incluir el no pago de deudas originadas de relaciones contractuales.

8. SITUACIÓN DEL ORDENAMIENTO JURÍDICO VENEZOLANO

En diciembre de 1999 entró en vigencia la nueva Constitución de la República Bolivariana de Venezuela, en cuyo artículo 28 se consagró el *habeas data* como un derecho fundamental y de naturaleza jurídica propia, distinto al derecho a la protección a la intimidad y vida privada determinado en el artículo 60; Ídem[21].

En ese sentido, el referido artículo 28 expresa: "Toda persona tiene el 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 de 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".

El contenido del artículo 28 transcrito puede dividirse en dos aspectos. Por un lado, se garantiza constitucionalmente la protección de los datos personales como un derecho de carácter fundamental, ya que se establece la posibilidad real

20 Declaración de Cartagena de Indias, III Encuentro Iberoamericano de Protección de Datos, 25-28 de mayo de 2004.

21 El artículo 60 de la Constitución de la República Bolivariana de Venezuela dispone: "Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. 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".

del control del uso y finalidad a que se destina la información relativa a los datos personales y la posibilidad de oponerse a la utilización de los mismos, de tal forma de impedir que esa información sirva a propósitos rechazados por el titular. Así, nos encontramos con un "derecho autónomo no mediático que se basta a sí mismo sin necesidad –de– que –el tratamiento de– la información o los datos sean lesivos de otros bienes constitucionales[22]".

Por el otro lado, la misma disposición constitucional determina la vía judicial como el camino procesal a seguir para hacer valer ese derecho a la protección de datos personales, sin condicionar o supeditar su ejercicio a una solicitud extrajudicial previa. De esa forma el contenido del artículo 28 de la Constitución de la República Bolivariana de Venezuela no puede ser entendido únicamente como un recurso para hacer efectivo el derecho a la intimidad, sino como la consagración del derecho fundamental a la protección de datos personales.

Sin embargo, hasta la presente fecha no existe el cuerpo normativo de rango legal que desarrolle el derecho consagrado en la disposición constitucional citada, lo cual no puede ser interpretado como una imposibilidad para el ejercicio del mismo, ya que, de conformidad con lo dispuesto en el artículo 22 de la misma Constitución venezolana[23], la falta de dicho instrumento legal no menoscaba su ejercicio, pero, sin duda, sí dificulta su pleno disfrute.

Ante la falta de una ley de protección de datos ha sido la Sala Constitucional del Tribunal Supremo de Justicia la encargada de determinar el alcance y contenido del derecho a la protección de datos personales. Así, en sentencia 0332 del 13 de marzo de 2001, expediente 1797, dicha Sala Constitucional expresó que del contenido del artículo 28 de la se infiere el derecho que tiene toda persona natural o jurídica de recopilar información sobre otras personas sin ningún tipo de límites fijados en esa propia norma, pero que su ejercicio no puede atentar contra el derecho a la intimidad y vida privada contenido en el artículo 60 del mismo cuerpo constitucional, que el *habeas data* corresponde tanto a personas naturales como jurídicas, y además precisó el procedimiento a seguir para hacerlo valer.

Ahora bien, no se puede compartir la precisión de la Sala Constitucional relativa al derecho ilimitado de recopilar datos sobre los demás, que emana implícitamente del contenido del artículo 28 ya que dicha actividad se encuentra limitada por el contenido de la propia disposición constitucional y de los principios que lo informan. Así, el citado artículo consagra el derecho de rectificación de la información recopilada, que implica necesariamente un límite al tratamiento de datos reflejado en

22 ORTÍZ-ORTÍZ. Ob. cit., 215.

23 El artículo 22 de la Constitución de la República Bolivariana de Venezuela consagra: "La enunciación de los derechos y garantías contenidos en esta Constitución y en los instrumentos internacionales sobre derechos humanos no debe entenderse como negación de otros que, siendo inherentes a la persona, no figuren expresamente en ellos. La falta de ley reglamentaria de estos derechos no menoscaba el ejercicio de los mismos".

la exigencia de la calidad en la recolección de los mismos y, a su vez, nos encontramos con el principio informador relativo al consentimiento del titular de los datos, cuya inexistencia acarrea la ilegalidad de dicha recolección o tratamiento.

Incluso, la anterior posición de la Sala Constitucional del Tribunal Supremo de Justicia venezolano, en relación con el supuesto derecho ilimitado de recolección de datos personales, no encuentra apoyo en el anteproyecto de Ley de Protección de Datos y Habeas Data para Venezuela, que establece los límites al ejercicio de esa actividad cuando dispone que "los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido"[24], y que "es ilícito el tratamiento de datos personales cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias"[25].

También es necesario disentir de la afirmación de la Sala Constitucional en relación con que el tratamiento de datos personales no debe quebrantar el derecho a la protección a la intimidad y a la vida privada contenida en el artículo 60 de la Constitución, ya que aceptar la misma sería otorgar un mero carácter instrumental del derecho de protección de datos personales, que implicaría que su denuncia requeriría de la infracción de otros derechos constitucionales, lo cual no es cierto. Lo que debe respetar el tratamiento es el derecho a la protección de datos personales como derecho autónomo e independiente al de la protección a la intimidad y vida privada[26].

En cuanto a la posibilidad de aplicar esta protección a las personas jurídicas, parece más apropiado el criterio asumido por la Agencia Española de Protección de Datos en el sentido de que dichos entes carecen de intimidad y vida familiar, lo que no excluye su protección por otras vías[27].

Una observación adicional es necesario realizar en cuanto al criterio de la Sala Constitucional del Tribunal Supremo de Justicia, y es la relativa al procedimiento a

24 Artículo 5 del anteproyecto de Ley de Protección de Datos y Habeas Data para Venezuela.

25 Artículo 8 del anteproyecto de Ley de Protección de Datos y Habeas Data para Venezuela.

26 Esta posición encuentra sustento en el artículo 1 del anteproyecto de Ley de Protección de Datos y Habeas Data para Venezuela, que a la letra expresa: "La presente Ley tiene por objeto garantizar y proteger íntegramente los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, tanto públicos como privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 28 de la Constitución Nacional".

27 No obstante, y a pesar del criterio de que las personas jurídicas carecen del derecho a la protección de datos, sustentado en el presente trabajo, es oportuno recordar que la legislación de Argentina, al igual que el anteproyecto venezolano, extiende esta protección a las personas ideales o jurídicas.

seguir para hacer valer el derecho a la protección de datos personales mientras no sea aprobada la ley que desarrolle la disposición constitucional que lo consagra. En ese sentido, ha establecido la citada Sala que los derechos determinados en el artículo 28 de la Constitución podrán hacerse valer mediante una acción autónoma de amparo constitucional ante el tribunal competente de acuerdo a la materia, siempre y cuando se cumplan las exigencias legales para ello. De lo contrario, es decir, cuando no se encuentren cumplidas las exigencias para el amparo constitucional, deberá interponerse una acción autónoma de *habeas data* ante la propia Sala Constitucional, la cual se tramitará de acuerdo al procedimiento establecido en el propio auto de admisión[28].

Ahora bien, a pesar de la inexistencia de una ley que desarrolle el derecho constitucional a la protección de datos personales establecido en el artículo 28 de la Constitución, dentro del ordenamiento jurídico venezolano existen normas que tienden a proteger dichos datos personales, pero en salvaguarda del derecho de protección a la intimidad y vida privada, al trabajo, y a la libertad de empresa, entre otros.

En ese sentido podemos mencionar la Ley de Protección al Consumidor y al Usuario, dentro de la cual, y con ocasión de la regulación del comercio electrónico, se dispone, en relación con la publicidad electrónica, la obligación del proveedor de proporcionar mecanismos a los consumidores para limitar la recepción de mensajes comerciales (Antispam)[29]. También se determina la obligación del proveedor de establecer los dispositivos necesarios que garanticen la privacidad de los consumidores o usuarios que hagan uso de los bienes y servicios ofertados por cualquier medio electrónico, de forma tal que la información intercambiada no sea inteligible para terceros no autorizados que tengan acceso a ella voluntaria o accidentalmente[30].

28 La Sala Constitucional del Tribunal Supremo de Justicia de Venezuela en sentencia 0332 del 13 de marzo de 2001 sostuvo: "Ha sido criterio de esta Sala, sostenido en fallos de 20 de enero y 1.º de febrero de 2000, que las normas constitucionales tienen vigencia plena y aplicación directa, y que cuando las leyes no han desarrollado su ejercicio y se requiere acudir a los tribunales de justicia, debido a la aplicación directa de dichas normas, es la jurisdicción constitucional, representada por esta Sala Constitucional, la que conocerá de las controversias que surjan con motivo de las normas constitucionales aún no desarrolladas legislativamente, hasta que las leyes que regulan la jurisdicción constitucional, decidan lo contrario".

29 En ese sentido el artículo 34 de la Ley de Protección al Consumidor y al Usuario determina: "Los proveedores deberán desarrollar e implantar procedimientos fáciles y efectivos que permitan al consumidor o usuario escoger entre recibir o no mensajes comerciales electrónicos no solicitados. Cuando un consumidor o usuario haya indicado que no quiere recibir mensajes comerciales electrónicos no solicitados tal decisión deberá ser respetada".

30 El artículo 37 de la Ley de Protección al Consumidor y al Usuario consagra: "En las negociaciones electrónicas, el proveedor deberá garantizarse la utilización de medios

Asimismo, la Ley de Igualdad de Oportunidades para la Mujer, en protección del derecho al trabajo, contempla una prohibición para las empresas de exigir a las solicitantes de empleo, o a sus trabajadoras, informes médicos que revelen un posible embarazo, con el fin de decidir sobre su contratación o continuación en el empleo[31]. De la misma manera, y en protección del mismo derecho al trabajo, la Ley de Registro de Antecedentes Penales prohíbe a cualquier empresa o persona exigir a un particular, como requisito para su contratación, la presentación de sus antecedentes penales[32].

Para finalizar, la Ley Especial contra los Delitos Informáticos, en resguardo de la vida privada, considera delito el apoderamiento, utilización, modificación, eliminación o cesión, sin el consentimiento de su dueño, de la información personal de otro que se encuentre incorporada en un computador o sistema que utilice tecnologías de información[33].

necesarios que permitan la privacidad de los consumidores o usuarios que hagan uso de los bienes o servicios ofertados por cualquier medio electrónico, 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 a ella voluntaria o accidentalmente. A este respecto, debe señalarse 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, los proveedores en las relaciones comerciales que se lleven a cabo a través de la utilización de medios electrónicos, podrán utilizar cualquier vía para garantizar la privacidad y confidencialidad de las relaciones, la cual deberá encontrarse ampliamente a la disposición de los consumidores o usuarios".

31 El artículo 24 de la Ley de Igualdad de Oportunidades para la Mujer señala: "El embarazo es una condición natural de la mujer y como tal no puede ser motivo de discriminación. Por lo tanto, las empresas se abstendrán de exigir o de practicar a las solicitantes de empleo o a las trabajadoras ya incorporadas en una empresa, exámenes médicos para descartar o comprobar un posible embarazo, con fines de aprobar o rechazar su ingreso o permanencia en dicha empresa. Tal acción será considerada como lesiva a los derechos laborales de la mujer, y en tal sentido, dará lugar a la solicitud del Recurso de Amparo correspondiente".

32 El artículo 8 de la Ley de Registro de Antecedentes Penales dispone: "Queda prohibido a cualquier empresa o persona, exigir a los particulares, con ocasión de las ofertas de trabajo y en materia relacionada con el reclutamiento laboral, la presentación de los Antecedentes Penales".

33 Los artículos 20 y 22 de la Ley Especial contra los Delitos Informáticos determinan: "Artículo 20. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias". "Artículo 22. El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aun cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad".

9. LOS CÓDIGOS DE CONDUCTA

Una posible solución para aquellas empresas ubicadas en Estados cuyos ordenamientos jurídicos no posean un nivel de desarrollo que garantice la protección de datos personales y por tanto no estén considerados como destino seguro, como es el caso de Venezuela, es la adopción de los denominados "códigos de conducta", que no son más que un cuerpo normativo asumido por una empresa o por grupos de ellas para regular su actividad.

Estos códigos de conducta "tienen el carácter de códigos deontológicos o de buenas prácticas y constituyen un instrumento propicio para potenciar el adecuado tratamiento de los datos personales, complementando o desarrollando los marcos regulatorios existentes"[34]. La forma más adecuada de asumir estos códigos por parte de la empresa es contemplando en los respectivos estatutos que la actividad de sus órganos estará regida, entre otras, por los códigos de conducta que se aprueben por el consejo directivo o por la corporación que la agrupe.

34 Declaración de Cartagena de Indias, III Encuentro Iberoamericano de Protección de Datos, 25-28 de mayo de 2004.