

LOS DERECHOS A LA INTIMIDAD Y A LA PRIVACIDAD EN VENEZUELA Y EN EL DERECHO COMPARADO*

por Flor María Ávila Hernández, Katia Castaldo y Anthony Urdaneta

Meza **

RESUMEN

Desde el punto de vista conceptual, en todas las legislaciones se habla de intimidad y privacidad como un solo concepto integrado, mientras que en nuestra legislación venezolana no es así. La privacidad se refiere a aquella parte del individuo que va más allá de lo íntimo, esto es, información que tomada por sí misma puede no ser relevante, pero que analizada en un contexto concreto puede conducir a la construcción de un perfil fiable del individuo.

En Latinoamérica se ha desarrollado ampliamente el *habeas data*. En la actualidad, no hay legislación que lo regule expresamente, a falta de ello, la Sala Constitucional del Tribunal Supremo de Justicia emitió una jurisprudencia donde se desarrolla la multidimensionalidad del derecho. En cuanto a la doctrina comparada, se encuentra unanimidad en que el *Habeas data* es una acción de carácter judicial, pero hay desacuerdo en cuanto a los derechos que tutela; una parte sostiene que el *Habeas Data* es un mecanismo que protege el espacio íntimo de las personas en cuanto a los datos almacenados en computadoras y la otra, sostiene que el *Habeas data* protege el derecho a la información y tutela la identidad del individuo frente a la sociedad.

PALABRAS CLAVE

Derecho a la intimidad, derecho a la privacidad, *habeas data*, información personal, constitución.

ABSTRACT

In a conceptual perspective, in all legislation it's mentioned intimacy and privacy as an integral concept, but in the Venezuelan legislation is not like this. Privacy protects a part of a person that is more away from intimacy, that is, information that may not be relevant by itself but analyse in a determinative context can construct a person profile.

In Latinoamerica it is broadly developed the *habeas data*. Actually, there is not legislation that regulates it categorically this juridical institution, The Constitutional Sale of The Supreme Court of Justice has created a jurisprudence where it's developed the multidimensional of the right. In the comparative law, it's unanimous that *habeas data* is a juridical law action, but scientists disagree in the rights that this institution protect; a part of the doctrine agrees that *Habeas data* is a mechanism that protects the intimate space of people, the personal data registered in computers and the other, agree that *Habeas data* protects the right to the information and protects the personal identity in front of society.

KEY WORDS

Right to intimacy, right to privacy, *habeas data*, personal information, constitution.

1. Introducción. Privacidad e intimidad. Nociones preliminares

Cuando se habla de la protección de datos como derecho fundamental se tiende a hablar de los términos "intimidad" y "privacidad" indistintamente. Sin embargo, estos dos términos tienen

* Fecha de recepción: 15 de marzo de 2007. Fecha de aceptación/publicación: 18 de julio de 2008.

** Flor Ávila es Abogada, Magister en CC. Políticas y Derecho Público, Doctora en Filosofía del los Derechos Humanos, Jefa de la Sección de Publicación y Divulgación del Instituto de Filosofía del Derecho J.M. Delgado Ocando de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia (Venezuela). Katia Castaldo es Abogada y Doctora en Derecho por la Universidad Federico II de Nápoles (Italia). Anthony Urdaneta es estudiante de 5º año de la Escuela de Derecho de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia (Venezuela).

un alcance distinto que es necesario conocer para saber dónde empiezan y acaban el derecho a la intimidad, a la privacidad y a la protección de datos de carácter personal.

De igual forma, ubicamos a los derechos a la privacidad e intimidad en el cuadro de una sociedad abierta o libre (en sentido popperiano), democrática y de la información o conocimiento como parte del desarrollo de la identidad personal y del libre desenvolvimiento de la personalidad al que tiene derecho toda persona conforme a su dignidad humana. Como señala Eusebio Fernández el concepto de dignidad humana gira en torno a “que cada uno de los seres humanos tiene un valor moral especial, que ha de ser reconocido y garantizado por las leyes y que significa, al mismo tiempo, el derecho a tener unos derechos básicos e inviolables” (Fernández, 2004: 40).

El alcance de los derechos a la privacidad e intimidad y su colisión con otros derechos constitucionales y con algunos valores morales son cuestiones filosófico-jurídicas de gran relevancia que interesa debatir y no se pueden soslayar en una sociedad democrática y de la información.

También estamos en presencia de una sociedad basada fuertemente en imágenes, especialmente de los individuos, donde la información privada, personal, es fundamental en la construcción de perfiles. En efecto, como afirma Sartori, en su libro *Homo viden*, “la premisa común sobre la que se basa de principio a fin es que el primado del ver, el primado de la imagen, empobrece el conocer y del mismo modo debilita nuestra capacidad de gestionar la vida en sociedad...” (Sartori, 2000: 161).

Es por ello que nos ocuparemos de ambos derechos. En efecto, el derecho a la intimidad protege la parte más íntima de una persona, esto es, esa esfera personal que define qué es y qué no es privado. Dicho de otra forma, hablar de intimidad es hablar de sentimientos, de creencias (políticas, religiosas), pensamientos o de una información, o la relativa a la vida sexual, cuya difusión puede producir ciertas reservas al individuo. Se trata en definitiva de aquellos datos que bajo ninguna circunstancia proporcionaría un individuo de manera libre y consciente.

La privacidad, sin embargo, es un término más amplio: se refiere a aquella parte del individuo que va más allá de lo íntimo, esto es, información que tomada por sí misma puede no ser relevante, pero que analizada en un momento o contexto concretos puede llevarnos a la construcción de un perfil muy fiable del individuo que permita su caracterización e identificación.

Existe un elemento que es común tanto en el concepto de intimidad como en el de privacidad: el tratamiento de la información personal. La información es, entonces, el elemento fundamental, la materia de la que están formadas privacidad e intimidad, según Santiago Battaner (2006).

2. Constitución Venezolana que prevén los derechos a la privacidad y a la intimidad.

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.

Artículo 48. Se garantiza el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso.

Artículo 60. 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.

3. El derecho de *habeas data*

El *habeas data* tiene entre sus antecedentes a la acción de *habeas corpus*. El vocablo "habeas" proviene del latín *habere*, que significa téngase en su posesión y "*data*", proviene del inglés que significa datos, definido por los diccionarios como representación convencional de hechos, conceptos o instrucciones de forma apropiada para la comunicación y procesamiento por medios automáticos. Por lo que "habeas data" quiere decir "téngase los registros, los datos".

En la doctrina comparada hay unanimidad en que la formulación "habeas data" se origina parcialmente en el *habeas corpus*, pero mucho se ha discutido con respecto a la significación de la palabra *data*. Con referencia a esta última existen dos vertientes,

una según la cual *data*, es un acusativo neutro plural de *datum*, de la misma raíz que el verbo latino *do, das, dedi, datum, dare*, "dar", "ofrecer". *Datum*, singular de *data*, es empleado con el sentido de presentes, donativos, ofertas y no con el sentido de datos. La vertiente contraria sostiene que la palabra *data* proviene del inglés, "posición que encuentra como fundamento el hecho de haber sido utilizado en tal sentido por la *Data Protection Act* inglesa, la *Data Lag* sueca, la *Federal Data Protection Act* austríaca, y otras... (Defensoría del Pueblo, 1998).

Varias definiciones se han dado con relación a esta acción. Es así como, en Argentina, se considera como una de las garantías constitucionales más moderna, definiéndose de la siguiente manera: "Una acción judicial para acceder a registros o bancos de datos, conocer los datos almacenados y en caso de existir falsedad o discriminación corregir dicha información o pedir su confidencialidad".

De lo antes expuesto podemos colegir que el *habeas data* es considerado como una posible acción judicial tendiente a permitir el acceso a los datos que se encuentran almacenados en registros, tanto públicos como privados, a los fines de controlar dicha información y, en caso de que dicha información sea falsa o discriminatoria, se podrá solicitar la supresión, rectificación, confidencialidad o actualización de ésta. Los motivos del *habeas data*, según la legislación citada, permite que sea dividido en dos etapas, el derecho al acceso y, posteriormente, el derecho a la supresión, rectificación o confidencialidad, en el supuesto de que sea falsa o errónea.

En cuanto al origen de esta acción, tenemos que las primeras Constituciones en abordar el tema sobre la problemática de la explosión informática fueron las de España (1978) y Portugal (1976), aunque realmente dichas disposiciones no establecieron acciones jurisdiccionales especializadas en proteger y combatir los efectos negativos del fenómeno informático. Es realmente a partir de los procesos constituyentes de los países latinoamericanos donde ha tenido mayor desarrollo esta institución, siendo en Brasil donde se puede localizar el origen de esta acción con este mismo nombre, en el artículo 5, numeral LXXII, de la Constitución de 1988, que reza: "Conceder el *habeas data*: a. Para asegurar el conocimiento de informaciones relativas a la persona de quien lo pide, que conste en registro o en banco de datos de entidades gubernamentales o de carácter público. b. Para la rectificación de datos, cuando no se prefiera hacerlo por procesos reservados judicial o administrativo".

A partir de dicha disposición, comienza a incorporarse dentro de las diferentes Constituciones latinoamericanas la acción del *habeas data*, ya sea con ese nombre o con uno diferente, o bien como un derecho. En este sentido, tenemos la Constitución de Colombia de

1991 (artículo 15) y la Constitución de Guatemala (artículo 31) que lo reconoce como una garantía y no como un proceso autónomo.

En la Constitución de Paraguay de 1992 (artículo 135) se reconoce como una acción con un procedimiento judicial especial, tendiente a la tutela o protección de los derechos establecidos en dicha norma. En Perú, en la Constitución de 1993 (artículo 200) se reconoce expresamente como una acción judicial con esa misma denominación, a diferencia de Argentina, en donde es introducida en la reforma constitucional de 1994 (artículo 43) tratándose como un subtipo especial de amparo.

En la doctrina argentina, si bien hay unanimidad en el tratamiento como una acción judicial, no existe en relación con su "filiación. En efecto, si bien la mayoría de los autores indican que se trata de un amparo especializado. Para otros se emparenta más con el hábeas corpus. (*omissis*) Al analizar la evolución histórica desde la creación del clásico habeas corpus, hasta el novísimo hábeas data, y distinguiendo entre ambos institutos, (...) se comprueba una inicial coincidencia en lo referente a su naturaleza jurídica. En ambos casos no se trata de derechos fundamentales, *strictu sensu*, sino de instrumentos o garantías procesales de defensa de los derechos a la libertad personal, en el caso del hábeas corpus, y de la libertad informática en lo concerniente al hábeas data". (Defensoría del Pueblo, 1998)

En el sentido divergente, es decir, entre los que tratan al hábeas data como un derecho o garantía, tenemos a Colombia, Chile, y Perú, en donde se concibe expresamente como una garantía. En estos ordenamientos jurídicos aparece como un derecho debido a su formulación constitucional, pero capaz de ser protegido por medio de procesos constitucionales específicos.

3.1. JURISPRUDENCIA VENEZOLANA

En Venezuela, debido a la inexistencia de una ley que desarrolle y regule el contenido del artículo 28 de la Carta Fundamental, la jurisprudencia ha regulado el hábeas data, estableciendo lo siguiente:

Este grupo de derechos, que emanan del artículo 28 constitucional, pueden ejercerse por la vía judicial, pero ellos no responden en principio a amparos constitucionales. El primero de ellos (derecho a conocer) es de naturaleza netamente inquisitiva, ajeno a la estructura que para el proceso de amparo señala el artículo 18 de la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales... Los derechos del artículo 28 constitucional, se ejercen mediante acciones autónomas, y ellos no se ejecutan como una modalidad del amparo, como lo sostienen Víctor Pedro Sagües

(*Acción de Amparo*. Buenos Aires: Astrea), o Augusto Morello (*Constitución y Proceso*. Buenos Aires: Abeledo Perrot) para el derecho argentino, así como lo hacen otros autores (*Habeas data*, por Alicia Pierini, Valentín Lorences y María Inés Tornabene. Buenos Aires: Editorial Universidad, 1999).

Por lo que en Venezuela es necesario que el legislador asiente la naturaleza jurídica de dicha institución, ya que de lo antes expuesto se colige que el hábeas data será cualquier tipo de procedimiento que tenga como finalidad acceder a una información para conocer su contenido, diferenciándolo así del amparo, pero al mismo tiempo, asimilándolo ante determinadas circunstancias.

En definitiva, estando el *hábeas data* regulado, a veces como un derecho-garantía o como una acción judicial, en definitiva va a ser decisión de cada país, a través de su ordenamiento jurídico interno apoyado por la jurisprudencia y doctrina, lo que va a determinar la tendencia a seguir a los fines de especificar, precisar y delimitar su naturaleza jurídica.

3.2. Objeto y finalidad

El *habeas data*, por tratarse de una institución relacionada con la informática y por consiguiente con la creación de archivos, registros y bases de datos, es menester establecer el objeto o la finalidad que se persigue con dicha institución. En un sentido literal, el *habeas data* parte de la idea inicial de la obtención de datos, pero es necesario aclarar cuáles datos son los que se pueden obtener, ya que se podría interpretar que sería con respecto a cualquier tipo de datos. Es así como, los datos a los cuales se pueden acceder son los datos personales que podrían ser vulnerados por informaciones de carácter público, en virtud de que la protección de la persona contra el uso abusivo de los datos contenidos en los registros o bases de datos es uno de los fines fundamentales que tiene esta institución jurídica.

Desde un punto de vista teórico, se podría considerar que el *hábeas data* está diseñado para proteger uno o más derechos, sin que ello llegue a implicar que éstos sean de su exclusividad, ya que existen otras figuras aptas para proteger derechos ante diferentes supuestos. En este sentido, tenemos que el derecho a la reparación de los daños o el derecho al control de las actividades de los bancos de datos pueden ser protegidos, pero por medio de otros procedimientos judiciales diferentes al *hábeas data*.

3.3. Derechos tutelados

En lo atinente a los derechos que se tutelan por medio de esta institución, la doctrina se encuentra dividida, ya que se ha sostenido que la tutela aludida se refiere, bien al derecho a la información, al derecho a la intimidad, al derecho a la identidad o al derecho a la autodeterminación informática. En este sentido, parte de la doctrina sostiene que, debido al nacimiento de la informática y con ella el procesamiento de datos, existe la posibilidad de registrar una gran cantidad de datos sobre las personas que permiten reconstruir sus detalles íntimos y con ello afectar su vida privada o intimidad. Dentro de este contexto, consideran al *hábeas data* como un mecanismo tendiente a proteger ese espacio íntimo de la persona, es decir, como una herramienta para defenderse de las intromisiones, tanto por parte del Estado como de los particulares. En este sentido, parte de la doctrina argentina relacionó "la indefensión de la persona frente al mal uso de sus datos y a la publicidad de los mismos, con el derecho constitucional a la privacidad" (Defensoría del Pueblo, 2008), así como consideran al *hábeas data* como una garantía al derecho a la privacidad y protege a las personas contra la discriminación. Dentro de esta postura, encontramos autores con una visión mucho más amplia, puesto que a consecuencia del derecho a la intimidad, consideran otra gama de derechos, entre ellos el derecho a la integridad, el derecho al trabajo, el derecho de acción sobre datos falsos, etc.

Sin embargo, otro sector de la doctrina, considera que la situación puede trascender del derecho a la intimidad, y por ende puede relacionarse con el derecho a la identidad. Cuando un sujeto intenta corregir los datos falsos que se encuentran almacenados en los bancos de datos o los registros, lo que se intenta realmente es tutelar la identidad del individuo frente a la sociedad. Igualmente encontramos, que parte de la doctrina comparada estima que el *hábeas data* protege el derecho a la información.

El *hábeas data* representa una nueva garantía constitucional, puesto que tutela la libertad informática y con ella el derecho a la autodeterminación informativa, entendiendo a éste último como "la facultad de la persona de decidir básicamente por sí misma cuando y dentro de qué límites procede revelar situaciones dentro de la propia vida".

Como se puede observar, el *hábeas data* tutela y protege una serie de derechos personalísimos, por lo que todo dependerá de la situación en particular, así como de la concepción que se tenga dentro de cada ordenamiento jurídico.

3.4. Criterios Jurisprudenciales del Tribunal Supremo de Justicia Venezolano

El Tribunal Supremo de Justicia, en sentencia de fecha 23 de agosto de 2000, estableció que el artículo 28 de la Constitución de la República Bolivariana de Venezuela tutela una serie de derechos reconocidos en ese mismo artículo en los siguientes términos:

"El artículo 28 de la vigente Constitución establece el derecho de las personas a conocer la información que sobre ellas, hayan sido compiladas por otras (omissis) Tanto el Estado, como los particulares, mediante diversas formas de compilación de datos: manuales, computarizados, etc., registran y almacenan datos e informaciones sobre las personas o sobre sus bienes, y en vista que tal recopilación puede afectar la vida privada, la intimidad, el honor, la reputación, la vida económica y otros valores constitucionales de las personas naturales o jurídicas, la Constitución, para controlar tales registros, otorga varios derechos a la ciudadanía que aparecen recogidos en el artículo 28 citado. Estos derechos son: 1) El derecho de conocer sobre la existencia de tales registros. 2) El derecho de acceso individual a la información, la cual puede ser nominativa, o donde la persona queda vinculada a comunidades o a grupos de personas. 3) El derecho de respuesta, lo que permite al individuo controlar la existencia y exactitud de la información recolectada sobre él. 4) El derecho de conocer el uso y finalidad que hace de la información quien la registra. 5) El derecho de actualización, a fin que se corrija lo que resulta inexacto o se transformó por el transcurso del tiempo. 6) El derecho a la rectificación del dato falso o incompleto. 7) El derecho de destrucción de los datos erróneos o que afectan ilegítimamente los derechos de las personas".

Como bien se puede observar, dentro de nuestro ordenamiento jurídico el hábeas data es considerado tanto un derecho como una acción. Si se parte de una concepción restringida, se podría concluir que será necesario que la Asamblea Nacional legisle sobre la materia para poder determinar los efectos de dicha acción, pero vía interpretación analógica, se puede concluir que se podría aplicar el procedimiento de amparo. En este sentido, en sentencia posterior, de fecha 14 de marzo de 2001, la Sala Constitucional del Tribunal Supremo de Justicia expresó que el artículo 28 de la Constitución de la República si bien establece una serie de derechos a favor de las personas, los efectos de todos estos derechos no es el restablecimiento de una situación jurídica lesionada, sino condenar o crear una situación jurídica como resultado de su ejercicio, por lo que el accionante, en principio, no estaría interponiendo amparos constitucionales, "(d)e allí que con relación a dicha norma se hace necesario individualizar los derechos en ella contemplados, y

determinar cuándo en base a ellos, se puede originar un amparo y cuándo no". (Tribunal Supremo de Justicia, 2008).

Sin embargo, en la mencionada sentencia, la Sala establece que dicho artículo se encuentra conformado por un doble derecho, a saber:

"1. El de acceder a la información y a los datos que sobre sí misma o sus bienes consten en registros oficiales o privados. 2. A conocer la finalidad y uso que da el compilador a esos datos e información.

Indudablemente, el sentenciador obvió la plenitud hermenéutica del ordenamiento jurídico, ya que en aquellos supuestos de lagunas legales el sentenciador debe acudir a la analogía (*analogia legis*), que consiste en aplicar a un supuesto de hecho no regulado la consecuencia jurídica de una norma cuyo supuesto de hecho es tan semejante desde el punto de vista jurídico, que puede afirmarse que existe la misma razón (*eadem ratio legis*) para atribuir a aquél la consecuencia jurídica de ésta; o bien a los principios generales del derecho (*analogia juris*) que son principios inducidos de una pluralidad de disposiciones jurídicas y que tienen una generalidad mayor que cada una de esas disposiciones. Es menester recordar que "quien aplica el Derecho tiene que encontrar por sí la norma pertinente, en tanto en cuanto no la haya determinado la ley. A esta labor se llama investigación del Derecho".

3.4. Amparo de derechos que nacen del artículo 28 de la Constitución

El Tribunal Supremo de Justicia ha establecido que el artículo 28 de la Carta Magna otorga en sentido amplio el derecho a acceder a la información y al conocimiento del fin, pero se trata de derechos que han de ser ejercidos previamente (incluso extrajudicialmente y tal vez hasta por vía administrativa en algunos casos) ante el recopilador real o supuesto, naciendo la lesión al titular de los derechos de ese ejercicio extrajudicial fallido (ante el órgano administrativo que controla el dato personal). Ante tal situación, la víctima puede optar entre un juicio ordinario para hacer valer su derecho negado, acumulando pretensiones, o bien por medio de un amparo si se dan los supuestos para su procedencia.

En este orden de ideas, concibe el Máximo Tribunal que para intentar un amparo con base en el artículo 28 *ejusdem* se debe fundar la demanda en la existencia cierta de un sistema de información que lleva una persona, dentro del cual existen datos e informaciones referentes al accionante (datos e informaciones en plural, es decir, varios que permiten delinear en alguna materia un perfil de la persona, o de sus bienes). Mediante el amparo se puede

ejercer el derecho a acceder ante la petición de acceso extrajudicial negado ilegítimamente y que se concreta judicialmente mediante una exhibición, en caso de que una lesión de la situación jurídica del accionante se va a consolidar irremediabilmente por la negativa del acceso.

En lo concerniente al derecho a conocer el uso y finalidad de la recopilación, no es en principio el amparo una acción que permite la satisfacción plena de este derecho, según el Alto Tribunal, ya que quien tiene la información es realmente quien en su fuero interno conoce para qué la maneja y cómo la va a usar, e indagar tal propósito, no es materia de amparo. Por ello considera la Sala Constitucional que la determinación del uso y finalidad de los datos se pondera sólo en el sentido de declarar legal o ilegal lo que realiza el recopilador, no siendo tal declaratoria motivo de amparo, sino de una acción ordinaria o autónoma de *habeas data*.

Asimismo, la acción tendiente al acceso y a la destrucción del ilegal contenido del registro pueden acumularse y ventilarse mediante un amparo, cuando exista prueba fehaciente de la existencia del registro y de que en él se guardan informaciones y datos sobre el accionante, como parte de su contenido, así como del uso o fin ilegal que se hace de ellas en perjuicio del actor, si es que ello origina en su situación jurídica una lesión que de inmediato va a convertirse en irreparable o una amenaza inminente de lesión.

4. El derecho a la privacidad al interior del cuadro normativo europeo

Un primer reconocimiento de un verdadero y propio derecho fundamental al respeto por la vida privada ha sido asegurado a nivel europeo a partir del 1950 con la adopción por parte del Consejo de Europa de la Convención para la Salvaguardia de los Derechos y de las Libertades Fundamentales.

El artículo 8 de tal Convención prevé, en efecto, el "derecho al respeto de la vida privada y familiar:"1. Toda persona tiene el derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.2. No puede haber injerencia de una autoridad pública en el ejercicio de tal derecho a menos que tal injerencia sea prevista por la ley y constituya una medida que, en una sociedad democrática, es necesaria para la seguridad nacional, para la pública seguridad, para el bienestar económico del país, para la defensa del orden y para la prevención de los delitos, para la protección de la salud o de la moral, o para la protección de los derechos y de la libertad de los demás."

Para una descripción más completa del contenido de tal derecho se deberá, todavía, atender la Resolución n° 428 (1970) adoptada por la Asamblea Parlamentaria del Consejo de Europa:

"El derecho a la intimidad – así recita la Resolución – consiste esencialmente en el derecho de vivir la propia vida con un mínimo de interferencias. Esto concierne la vida privada y familiar, la integridad física y moral, el honor y la reputación, a los fines de evitar de ser expuestos bajo una falsa luz, la no revelación de hechos irrelevantes y embarazosos, la publicación no autorizada de fotografías privadas, la protección contra el uso impropio de las comunicaciones privadas, la protección de la divulgación de las informaciones suministradas o recibidas por singulares confidenciales" (Resolución 428 del Consejo de Europa, 1970)

El derecho a la privacidad venía en tal modo a configurarse, en las intenciones del legislador europeo, como una verdadera y propia "línea de límite" además del cual la sociedad no podía entrometerse en los asuntos de una persona. La privacidad terminaba, por lo tanto, con ser entendida como una esfera privada excluyente de cualquier forma de divulgación, capaz de consentir al singular de gozar de una sensación de control sobre sí mismo y del ambiente circunstante. (European Data Protection Supervisor, 2005: 16).

La institución, así operada, de un tal primero y verdadero "derecho a la privacidad" no podía, todavía, agotar el campo de las intervenciones normativas. La inminencia de un desarrollo tecnológico siempre más invasivo hizo, en efecto, necesario una ampliación del espectro normativo de previsión y aplicación y una adecuación terminológica y sustancial. El desarrollo de las tecnologías informáticas, en el cuadro, siempre más imponente, de aquella que de sociedad industrial vendrá a configurarse siempre más como una sociedad de la información, comenzaba, en efecto, ya a partir de los años 80, a incidir profundamente sobre la esencia misma del derecho a la privacidad que "de barrera contra el acceso a la esfera privada" iniciaba siempre más a ponerse como un "poder de autodeterminación sobre las propias informaciones (datos) personales" y, entonces, a un verdadero y propio "derecho a la autodeterminación informativa" (Sartor, 2005).

El derecho a la privacidad terminaba, por lo tanto, irreversiblemente con el configurarse como "poder de control sobre la circulación de las informaciones personales más bien que como proyección de un indiferenciado y aproximativo interés al aislamiento" (Rodotà, 2004).

En el tiempo de la información tecnológica la privacidad enviste, en efecto, inevitablemente la libertad misma del ciudadano de

controlar las informaciones que lo refieren; control esencial para "evitar que los muchos beneficios de la sociedad de la información, las oportunidades de participación social que ella ofrece, vengán cubiertos por intereses particulares, o vanificados por usos impropios o que les falta actualización de las grandes bases de datos" (Rodotà, 2002).

Las nuevas tecnologías actuando sobre la información, parte integrante de todas las actividades humanas, individuales y colectivas, inciden, en efecto, profundamente sobre cada aspecto de la vida individual y social favoreciendo la interconexión y la convergencia, pero también arriesgando seriamente de comprometerse la integridad misma de la vida individual (Sartor, 2006).

La tutela de la privacidad ha mostrado, así, una siempre una más estrecha conexión a la tutela de la libertad personal y existencial mostrándose, la expresión privacidad hasta muy reductiva respecto a las exigencias que con esa venían invocadas y por esto, frecuentemente afianzada, si no sustituida por otros, cual aquella de "protección de los datos" (Rodotà, 2002: 19).

Otros instrumentos legislativos han, por lo tanto, coherentemente visto la luz al interior del contexto europeo, primero entre todos la Convención Europea para la Tutela de las Personas Físicas con relación al Tratamiento Automático de los Datos Personales adoptada en el 1981.

La Convención representa la primera verdadera respuesta del Consejo de Europa a los nuevos desarrollos en el sector de las tecnologías de la información y de la comunicación. Esa tiene el declarado objetivo de proponer un proyecto para la armonización de la protección de los datos en cada Estado signatario a los fines de reforzar las libertades personales y de consentir la libre circulación de los datos personales entre países. La Convención no confiere directamente derechos a los ciudadanos europeos, pero se dirige únicamente a los Estados miembros del Consejo de Europa. Su función principal ha sido aquella de alentar a los Estados con o sin una insuficiente protección de los datos a legislar en este campo y a iniciar un debate sobre el tema (Zerdick, 1995: 64). La formulación del texto de la Convención 108, como también la explicación suministrada en la relación explicativa de acompañamiento, precisa que la protección de los datos no se refiere solo la tutela de la vida privada y de la vida familiar, pero también los otros derechos y libertades fundamentales.

En el artículo 1 es claramente definido el objetivo de la Convención:

“El objetivo de esta Convención es aquel de garantizar a cada individuo (...) respeto por sus derechos y libertades fundamentales, y en particular su derecho a la privacidad, con relación al tratamiento automático de datos personales que lo relacionan” (“La protección de los datos”).

No obstante la Convención 108, que consentía a los Estados signatarios de excluir algunas categorías de datos del campo de aplicación de la Convención, muchas incongruencias entre los sistemas nacionales de reglamentación han quedado. Tal disparidad pareciera ya en los primeros años noventa incompatibles con el crecimiento de la Comunidad europea y de los flujos de información a nivel mundial. Iniciaba, por lo tanto, a madurarse la conciencia al interno de las instituciones europeas de la necesidad de un enfoque uniforme a nivel comunitario en la protección de los datos. (EDPS, 2005:18-19). En el 1990 la Comisión Europea ha, en efecto, adoptado un paquete de medidas dirigidas a garantizar una uniformidad a nivel del enfoque en la disciplina para la protección de los datos y a armonizar las disposiciones nacionales en este campo. El elemento principal era la propuesta de una directiva marco, que tenía dos objetivos principales:

a) tutelar los derechos fundamentales y las libertades de las personas físicas y en particular su derecho a la vida privada con relación al tratamiento de los datos personales; b) evitar obstáculos a la libre circulación de los datos personales en toda la Comunidad. La propuesta viene, sin embargo, rechazada y la Comisión fue obligada a releerla. Mientras tanto, todavía, la importancia atribuida a la política de armonización de la protección de los datos se hacía siempre más imponente e irreversible. Bajo el impulso de las fuertes presiones que se habían madurado, en el 1995 fue adoptada – seguidamente de la presentación al Consejo Europeo de la ponencia *Europe's way forward to the information society* por parte de un grupo europeo a un alto nivel guiado por el Comisario Bangemann – la Directiva 95/46/CE sobre la tutela de las personas físicas con relación al tratamiento de los datos a carácter personal y la libre circulación de tal datos. En ausencia de una base jurídica específica, esta directiva se basa en el artículo 95 del Tratado que instituye la Comunidad europea, relativo al acercamiento de las legislaciones en el cuadro del mercado interno (ex artículo 100 A). Tal directiva mira a garantizar la libre circulación entre los Estados miembros de los datos personales a través de la armonización de las disposiciones nacionales sobre la tutela de las personas físicas respecto al tratamiento de tales datos.

Dado que todos los datos personales pueden circular entre los Estados miembros, la directiva 95/46 impone en línea de principio el respeto de las normas de tutela de tales datos respecto a cualquier

tratamiento de estos últimos, como dispuesto de su art. 3. Según cuanto es previsto por la Directiva 95/46, hecha las excepciones de las derogaciones admitidas por su art. 13, cualquier tratamiento de datos personales debe ser conforme, de una lado, a los "principios relativos a la cualidad de los datos", enunciados al art. 6 de tal directiva y, del otro, a uno de los "principios relativos a la legitimación del tratamiento de los datos" elencados al artículo 7 de esta última.

Más en particular, los datos deben ser "relevantes para finalizar, determinantes, explícitos y legítimos" (art. 6, n. 1, lit. b), así como "adecuados, pertinentes y no excedentes" respecto a dichas finalidades (art. 6, n. 1, lit. c). Además, según el art. 7, literales c y e, de la misma directiva, el tratamiento de datos personales es lícito respectivamente donde ese "[sea] necesario para cumplir una obligación legal a la cual es sujeto responsable del tratamiento" o "[sea] necesario para la ejecución de una tarea de interés público o conectado al ejercicio de los poderes públicos del cual ha sido investido el responsable del tratamiento (...) al cual vienen comunicados los datos".

En cuanto al objeto de la Directiva, esa se aplica a "cualquier operación o serie de operaciones seguidas sobre los datos personales", el llamado "tratamiento" de los datos. La Directiva se aplica también a los datos tratados mediante medios automatizados así como a los datos que hacen parte o que se prevé harán parte de "sistemas de registro" no automatizados en el cual esos son accesibles con base a criterios específicos. La Directiva sobre la protección de los datos no se aplica, en cambio, a los datos tratados por motivos puramente personales o actividades domésticas. Objeto de la directiva es, como arriba recordado, garantizar que los datos personales de todos los ciudadanos gocen de una protección equivalente en toda la Unión. A los veintisiete Estados miembros de la Unión Europea le ha sido solicitado de adecuar la propia legislación nacional a las disposiciones de la Directiva hasta el 24 de octubre de 1998.

La protección de los datos personales, como prevista por la Directiva 95/46, ha sido sucesivamente extendida también al sector de las comunicaciones electrónicas por medio de la Directiva 97/66/CE, sobre la Privacidad y las Comunicaciones Electrónicas, que se ha ocupado específicamente de la protección de la vida privada en el campo de las telecomunicaciones. Tal directiva afirma que los Estados miembros deben garantizar la privacidad de la comunicación a través de las normas nacionales. Entonces significa que la escucha, la interceptación, la memorización u otros tipos de interferencia o vigilancia de las comunicaciones, no autorizadas, son ilícitas. Allí donde sea prevista la identificación de la línea que llama, a los

usuarios debe darse la posibilidad de no adherir a tal servicio o no revelar la propia identificación al momento de una llamada. Por el contrario, los abonados a este servicio deben tener la posibilidad de rechazar las llamadas provenientes de personas que hayan desactivado la identificación de la propia línea llamante. La Directiva establece además que, allí donde existan repertorios de telecomunicaciones electrónicos o impresos, las personas tienen la facultad de ser omitidos del elenco, teóricamente en vía gratuita. La Directiva adoptada en el 1997 ha sido sustituida en el 2002 por una versión actualizada, la Directiva 2002/58 relativa a la vida privada y a las comunicaciones electrónicas. El objetivo es aquel de reglamentar las zonas que no han sido suficientemente cubiertas por la Directiva sobre la protección de datos, por ejemplo, el acceso a los datos de facturación, actividad de marketing, etc. La directiva del 2002 refleja la evolución de los mercados y de las tecnologías por los servicios de comunicación electrónica, como Internet, en modo de suministrar un igual nivel de tutela de los datos personales y de la vida privada, independientemente de las tecnologías usadas. Esa hacía parte de un grupo de 5 directivas y una decisión destinada a reformar el cuadro normativo existente para los servicios de comunicación electrónica y las redes de la Comunidad. Uno de los objetivos de esta reforma global era de crear reglas tecnológicamente neutrales, es decir, garantizar que los servicios sean reglamentados en manera equivalente, a prescindir de los medios tecnológicos del cual son consignados.

Por su parte, como afirma Molina Quiroga, Eduardo, y a los fines de completar la protección, para evitar la discriminación de personas, la Directiva 95/46 de la CE ha consagrado el derecho que tienen las personas a "no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc."

4.1. La contribución de la Corte Europea de los Derechos Humanos

La Corte de Estrasburgo ha sido desde siempre uno de los tribunales más atentos al desarrollo del nuevo modelo interpretativo relativo a la privacidad, acogiendo la idea de un derecho relacionado a la identidad personal y a la autodeterminación del individuo. La referencia al derecho al respeto de la vida privada ha sido, en efecto, más veces utilizado por la Corte para reprimir incriminaciones penales e interceptaciones telefónicas ilegítimas al igual de una serie de interferencias en la organización de la vida familiar y afectiva de las personas. A la tutela de la vida privada. la Corte Europea de los Derechos Humanos ha reconducido el derecho de mantener los

vínculos personales (CEDU C. c. Belgio 7.8.1996), el derecho al nombre (CEDU Burghartz v. Svizzera 22.2. 1994, CEDU Stjerna c. Finlandia 25.11. 1994), el derecho a la protección de los datos personales que se relacionan con la vida privada (CEDU Leander c. Svezia 17.5.1985) o menos (CEDU Rotaru v. Romania 4.5.2000).

El artículo 8, 1º coma de la Convención Europea para la Salvaguardia de los Derechos Humanos y de las Libertades Fundamentales, de conformidad con que "*cada persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*" ha permitido a la Corte Europea de Los Derechos Humanos de determinar, y progresivamente ampliar, el significado a asignar a los conceptos de "vida privada" y "correspondencia" (CEDU, Sentencia Malone c. Reino Unido, 2 agosto 1984 (corte plenaria) serie A n.82; Sentencia Gaskin c. Reino Unido, 7 julio 1989, corte plenaria, serie A n.160; Sentencia Z. c. Finlandia, 25 febrero 1997.), sentando así las bases de la positivización de un derecho al control consciente sobre cada forma de circulación de las propias informaciones personales.

Según la jurisprudencia de la Corte europea de los Derechos Humanos, y, sucesivamente, de la Corte de Justicia y del Tribunal de primer grado, el área cubierta por el término privacidad es, en efecto, de interpretar en sentido amplio – comprendiendo la protección de la vida privada, pero extendiéndose también más allá de esa – más bien que *stricto sensu*. Los jueces han así claramente optado por una interpretación del derecho a la privacidad que llegase a comprender la tutela también del derecho a la identidad y al desarrollo personal, así como el derecho para cada individuo de tomar y desarrollar relaciones con sus similares y con el mundo externo. La Corte europea de los Derechos Humanos tiene, además, claramente optado por un concepto de "vida privada" que comprenda privados, empresas, entes públicos o cualquier otro ambiente.

La Corte ha subrayado también muchas veces la correspondencia de esta interpretación extensiva con aquella de la Convención del Consejo de Europa del 28 enero 1981 para la Protección de los Individuos, con relación al tratamiento automatizado de los datos personales, entrada en vigor el 1º de octubre de 1985 y, cuya finalidad es, como ya hemos recordado arriba,

"garantizar (...) a cada individuo (...) el respeto de sus derechos y de las libertades fundamentales y en particular el derecho a la privacidad, respecto al tratamiento automatizado de los datos personales que lo afectan (artículo 1), donde tales datos son definidos en el artículo 2 como "cada información relativa a una

persona identificada o identificable" (sentencia Amann c. Svizzera (GC), n. 27798/95, párrafo 65, ECHR 2000 - II).

Además en la sentencia Peck/Regno Unito la Corte ha precisado: "Existe, entonces, un área de interacción entre el individuo y los terceros que, también en un contexto público, puede terminar con el reentrar en la esfera de la «vida privada»" (Corte europea de los Derechos Humanos, sentencia 28 enero 2003, Peck/Reino Unido, Recueil des arrêts et décisions, 2003-I, § 57).

El 27 de julio de 2004, además, con la sentencia del caso Sidabras vs. Lituania (Corte Europea de los Derechos Humanos, Segunda sección, Caso Sidabras and Džiautas vs. Lithuania, instancias n. 55480/00 e 59330/00.), la Corte Europea de los Derechos Humanos, dando una interpretación muy extensiva del derecho a la privacidad previsto en el artículo 8 de la Convención Europea de los Derechos Humanos, ha considerado que la tutela prevista por este artículo se extienda hasta comprender el derecho de cada uno de desarrollar relaciones sociales al reparo de cada forma de discriminación o estigmatización social, así consintiendo también el pleno goce de su vida privada. La Corte ha entonces considerado la compleja colocación de la persona en la sociedad, afirmando que el pleno respeto de la privacidad es una condición para la igualdad y el goce de los derechos fundamentales, como aquel del trabajo. (Stefano Rodotà, *Relazione 2004 Autorità Garante per la protezione dei dati personali*, Roma, 9 Febbraio 2005.)

Como hemos arriba recordado, también la Corte de Justicia ha optado por una interpretación extensiva del derecho a la privacidad refiriéndose, a tal fin, expresamente a la pertinente jurisprudencia de la Corte Europea de los Derechos Humanos.

En *Österreichischer Rundfunk* y otros, la Corte de Justicia ha, en efecto, confirmado que, por cuanto se refiere a un acto que entra en el campo de aplicación del derecho comunitario, el concepto de vida privada no debe ser interpretado en modo restrictivo, debiendo considerarse cual verdadero y propio "derecho fundamental". (Corte de Justicia, 2003).

"las disposiciones de la Directiva 95/46, dado que disciplinan el tratamiento de los datos personales que pueden traer perjuicio a las libertades fundamentales y, en particular, el derecho a la vida privada, deben ser necesariamente interpretadas a la luz de los derechos fundamentales, que según una constante jurisprudencia hacen parte integrante de los principios generales del derecho comunitario cuales la Corte garantiza la observación (v., señaladamente, sentencia del 6 marzo 2001, causa C-274/99 P, *Connolly/Commissione*, Racc. pag. I-1611, punto 37).

Tales principios han sido expresamente tomados por el artículo 6, n. 2, UE, en el sentido del cual "la Unión respeta los derechos fundamentales, como son garantizados por la [CEDU] y cuales resultan de las tradiciones constitucionales comunes de los Estados miembros, en cuanto principios generales del derecho comunitario".

4.2. El Garante europeo para la Protección de los Datos

El Tratado de Amsterdam, firmado el 2 de octubre de 1997 que entró en vigor el 1 de mayo de 1999, ha introducido al interno del Tratado CE un nuevo artículo 286.

El artículo consta de dos párrafos que prevén respectivamente:

Desde el 1º de enero de 1999 los actos comunitarios sobre la protección de las personas físicas con relación al tratamiento de los datos personales se aplican a las instituciones y a los órganos comunitarios;

Dentro de tal fecha el Consejo instituye un órgano de control independiente encargado de vigilar la aplicación de dichos actos a las instituciones y a los órganos comunitarios.

El artículo 286 implica, entonces, que la Directiva 95/46/CE, dirigida a los Estados miembros, y los otros actos comunitarios en materia de protección de los datos personales se aplican automáticamente a las instituciones y a los órganos comunitarios. Objeto de la disposición es garantizar que los datos personales sean igualmente protegidos a nivel de la Comunidad y de los Estados miembros (EDPS, 2005: 22) .

Con el reglamento n. 45/2001/CE del 18 diciembre 2000, concerniente a la tutela de las personas físicas en relación al tratamiento de los datos personales por parte de las instituciones y de los organismos comunitarios, así como la libre circulación de tales datos. El Parlamento Europeo y el Consejo han dado actuación al artículo 286. Tal reglamento contiene normas sustanciales sobre la protección de los datos dirigidos a las instituciones y a los organismos comunitarios, equivalentes a aquellos que la directiva 95/46/CE dada en relación a los Estados miembros. Según su artículo 3, ese se aplica al tratamiento de los datos personales por parte de todas las instituciones y de todos los organismos comunitarios, en la medida en la cual dicho tratamiento viene en el ejercicio de actividades que entran en todo o en parte en el campo de aplicación del derecho comunitario (Hijmans, 2006:1313).

El segundo coma del artículo 1 y el Capítulo V del Reglamento n. 45/2001 prevén, además, la introducción del Garante Europeo para la Protección de los Datos (GEPD) □ fenómeno, nuevo al interior del cuadro institucional de la Comunidad europea. El garante es nominado de común acuerdo por el Parlamento Europeo y por el Consejo por un periodo de 5 años, en base a un elenco predispuesto por la Comisión después de una invitación pública a presentar candidaturas.

Un garante agregado es nominado con el mismo procedimiento y por la misma duración, con la tarea de asistir al garante en el ejercicio de sus funciones y de sustituirlo en caso de ausencia o impedimento. Sin embargo, el reglamento que ha entrado en vigor en febrero del 2001, el primer Garante ha asumido el cargo solo el 17 de enero de 2004, fecha en la cual su nomina se ha transformada en ejecutiva. Instituido como autoridad independiente, el GEPD, a norma del artículo 41 del reglamento (CE) n. 45/2001, tiene la tarea de garantizar el respeto de los derechos y de las libertades fundamentales de las personas físicas, signadamente el derecho a la vida privada, por parte de las instituciones y de los organismos comunitarios en el sector del tratamiento de los datos personales. El GEPD desarrolla esencialmente tres funciones principales:

a. Control: asegurar y vigilar el cumplimiento, por parte de las instituciones y organismos CE, de sus obligaciones en materia de protección de datos, vigilar y asegurar el respeto de las disposiciones del Reglamento (CE) n. 45/2001, así como de cualquier otro acto comunitario relativo a la tutela de los derechos y de las libertades fundamentales, cuando las instituciones u organismos comunitarios tratan los datos personales («control»);

b. Consultación: suministrar asesoría a las instituciones y a los organismos CE en relación a cualquier argumento relativo al tratamiento de datos personales, comprendida la consultación en mérito a propuestas de ley y la vigilancia de los nuevos desarrollos que tienen una incidencia sobre la protección de los datos personales;

c. Cooperación: colaborar con las autoridades nacionales de control y con los órganos de control en el cuadro de la «tercera columna» de la Unión Europea para hacer más coherente la protección de los datos personales (EDPS, 2007: 13).

5. Conclusiones y Recomendaciones

Una conclusión de este breve itinerario acerca del significado y el alcance del derecho a la privacidad tanto en la perspectiva venezolana como comparada, no puede faltar de subrayarse en cuanto el derecho a la privacidad, las dimensiones y las modalidades de su tutela, se ligan en manera imprescindible, y también en sus diversos contextos socio-normativos, con la siempre más difusa

conciencia social de la necesidad de una mayor atención hacia una adecuada tutela de la persona contra las siempre nuevas lesiones de la esfera individual de parte sea de los individuos sea de los poderes públicos "El derecho a la privacidad" ha asumido, en este sentido el papel de un prisma mediante el cual se pueda recabar la imagen de la sociedad, que reclama urgentemente la tutela y sucesivamente ha forjado las formas.

LISTA DE REFERENCIAS

Battaner, S., 2006: «Intimidad, privacidad y protección de datos de carácter personal», *Baquia. Knowledge Center*, en www.baquia.com/noticias.php?id=10620

Defensoría del Pueblo, 2008: *La acción de habeas data*. DDG-167-01/16-07-2001:

<http://www.defensoria.gob.ve/detalle.asp?sec=160407&id=120&plantilla=1>.

European Data Protection Supervisor, 2005a: *Public access to documents and data protection*, Background Papers Series.

— 2005b: *The EDPS as an advisory to the community institutions*, Bruxelles.

— 2006: *Annual Report 2005*, Luxembourg .

— 2007: *Annual Report 2006*, Luxembourg.

Fernández, E. (2004) «Libertad de Expresión y Respeto a los Seres Humanos». *Revista Telemática de Filosofía del Derecho*. N°. 7, 2003/2004, pp. 39-55.

Hijmans, H., 2006: «The European Data Protection Supervisor: the institutions of the EC controlled by an independent authority», en *Common Market Law Review*, Vol. 43.

Molina Quiroga, E., 2008: «La elaboración de perfiles en la Ley 25.326», www.habeasdata.org

Rodotà, S., 2002: *Discorso tenuto dal Presidente nel giorno della presentazione della relazione sull'attività del Garante per l'anno 2001*, Roma 8 mayo 2002.

Rodotà, S., 2004: *Privacy, dignità, libertà. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, Wroclaw, Septiembre 2004.

Rodotà, S., 2005: *Intervista su privacy e libertà*. Roma-Bari.

Sartor, G., 2005: «Privacy, reputazione, e affidamento: dialettica e implicazioni per il trattamento dei dati personali», en: Pagallo U. (a cura di), *Privacy digitale: Giuristi ed informatici a confronto*, Torino 2005.

Sartor, G., 2006: *Informatica giuridica*: www2.cirsfid.unibo.it

Sartori, G., *Homo videns. La sociedad teledirigida*, trad. A.Díaz, Taurus, Madrid, 2000.

Zerdick, T., 1995: «European aspects of data protection, what rights for the citizen?», *Legal Issues of European Integration*, 2.

European Integration, 2.