CORTE SUPREMA DE JUSTICIA

PROTECCIÓN DE DATOS PERSONALES

DIVISIÓN DE INVESTIGACIÓN, LEGISLACIÓN Y PUBLICACIONES
CENTRO INTERNACIONAL DE ESTUDIOS JUDICIALES

ASUNCIÓN – PARAGUAY
2010

CORTE SUPREMA DE JUSTICIA

PROTECCIÓN DE DATOS PERSONALES

División de Investigación, Legislación y Publicaciones
Centro Internacional de Estudios Judiciales

ASUNCIÓN - PARAGUAY
2010

Alonso y Testanova. Asunción – Paraguay

Primera Edición: 500 ejemplares

Queda hecho el depósito que marca la Ley.

345.73 COR	Corte Suprema de Justicia – División de Investigación, Legislación y Publicaciones. Protección de Datos Personales Asunción – Paraguay. Edición 2010. 300p.

ISBN 978-99953-41-05-3

COORDINACIÓN:
VÍCTOR MANUEL NÚÑEZ RODRÍGUEZ, Ministro. Director

ELABORACIÓN DE LA OBRA
ROSA ELENA DI MARTINO.

APORTE DOCTRINARIO
ADRIANA RAQUEL MARECOS GAMARRA.

EDICIÓN:
MARCOS C. VILLAMAYOR HUERTA.

CORTE SUPREMA DE JUSTICIA

RAÚL TORRES KIRMSER
Presidente

VÍCTOR MANUEL NÚÑEZ RODRÍGUEZ
Vicepresidente 1º

SINDULFO BLANCO
Vicepresidente 2º

MIGUEL ÓSCAR BAJAC
ANTONIO FRETES
CÉSAR GARAY
ALICIA PUCHETA DE CORREA
Ministros

ÍNDICE:

INTRODUCCIÓN

INTRODUCCIÓN

Negar que la globalización de los mercados haya sido potenciada por la globalización de las redes telemáticas de comunicación, de naturaleza interactiva es una necedad y dentro de dicha globalización, Internet constituye la máxima expresión de la globalización. Ya sea que el proceso se denomine *globalización* o *mundialización*, entenderlo como un proceso meramente económico o financiero a escala mundial es insuficiente; este fenómeno influye sobre aspectos íntimos y personales de la vida de los sujetos del Derecho, rediagramando esquemas de la tradicional concepción del derecho a la intimidad, en particular, y de los derechos humanos, en general.

El Siglo XXI está dominado por el paradigma de la competitividad y el conocimiento, que se expresa en nuevas formas de producción, distribución y comercialización de bienes y servicios. En este paradigma, los recursos claves son la información y el conocimiento. Este paradigma está caracterizado, también, por el predominio de nuevas tecnologías como la automatización, la microelectrónica, la informática, los nuevos materiales y la biotecnología.

La disponibilidad de recursos naturales no garantiza, por sí sola, a ningún país el logro de las metas del desarrollo. Se deberá contar, además, con los conocimientos necesarios para el aprovechamiento, conservación y potenciación de tales recursos naturales. Las tecnologías facilitan el acceso y aseguran la acumulación del conocimiento. Específicamente, las tecnologías de la información y de las comunicaciones son el vehículo del acceso al conocimiento. El aprendizaje, proceso fundamental de las sociedades basadas en el conocimiento, busca la creación y fortalecimiento de capacidades y habilidades para el manejo de la información y del conocimiento, como factor dinamizador del cambio en la sociedad y en las empresas.

La República del Paraguay estará capacitada para superar las diferencias y las brechas económicas y sociales existentes si logra hacer del conocimiento un factor de cambio social y de competitividad. La modernización de la Administración Pública

demanda una nueva cultura basada en la innovación y en una mayor responsabilidad de por parte de Administración y administrados para con la sociedad, el medio ambiente y la calidad.

A lo largo de su vida, la persona va dejando un sendero, conformado por datos aislados que se van interrelacionando, de manera a brindar significados e interpretaciones diversas, creándose un perfil de ella, que la Ley está obligada a proteger; de esta forma, se ejerce un control social que interfiere en la vida humana, sin que los sujetos se percaten siquiera del mismo, de tal forma que las libertades y garantías consagradas por la Constitución Nacional colisionan con la convivencia diaria. Cuanto más avanza la *sociedad de la información*, más se sabe, cada día, acerca de nosotros.

Los nuevos adelantos tecnológicos tienen, como todo avance, aspectos positivos y negativos. Como medios aptos para la diseminación y captación generalizada de información, el desarrollo de los pueblos y el ejercicio de los más variados derechos, ha llamado la atención y, desde luego, provocado el apoyo de la comunidad internacional. Sin embargo y, dado que también puede provocar perjuicios a las personas, normas de diversas fuentes, han intentado establecer ciertos límites a la libertad de buscar, colectar y difundir información, a fin de lograr el respeto de los derechos y la protección de la seguridad nacional, del orden público, la moral y las buenas costumbres.

La capacidad de registro de las computadoras, la rapidez de consulta y de transferencia de datos y la cobertura de toda esa información genera, en la actualidad, para quien la posee o puede acceder a ella una fuerte dosis de poder, que puede ser tanto de poder económico, como de poder político, debido a que conocer minuciosamente la vida de los demás permite, en buena medida, regular controlar y vigilar su comportamiento.

Sostiene Emilio Del Peso, que la palabra *privacidad* es de uso corriente en el mundo jurídico y poco a poco se va diferenciando entre lo que es intimidad y lo que es privacidad[1] y, citando a Miguel

[1] DEL PESO NAVARRO, Emilio. *La protección de Datos y la Privacidad en Internet*, en INFORMÁTICA Y DERECHO Nº 33. INTERNET Y COMERCIO ELECTRÓNICO. UNED. Centro Regional de Extremadura. Mérida, 2000; pág. 64.

Ángel Davara, puede definirse *privacidad* como término al que podemos hacer referencia bajo la óptica de la pertenencia de los datos a una persona –su titular- y que en ellos se pueden analizar aspectos que individualmente no tienen mayor trascendencia, pero que al unirlos o otros pueden configurar un perfil determinado sobre una o varias características del individuo, que éste tiene derecho a exigir que permanezcan en su esfera interna, en su ámbito de privacidad"[2].

El dato es la noticia, el antecedente cierto que sirve como punto de partida para la investigación de la verdad. Es difícil –pero no imposible- que un dato aislado ponga en peligro la intimidad de las personas, ahora, cuando hablamos de *información*, es otra cosa porque ella está conformada por datos, que fueron objeto de un tratamiento que propició una estructura tal, que ostenta el carácter de información[3].

Es posible afirmar que la protección jurídica a la intimidad personal, debe equilibrar perfectamente la libertad y la convivencia y que deben ser arbitrados los medios jurídicos correspondientes para la protección de la vida privada, creando un marco de seguridad, defendiendo la intimidad, como derecho primordial del hombre, y tan antiguo como él mismo, para evitar su avasallamiento, a causa de la irrupción de las nuevas tecnologías para la información, procesamiento y entrecruzamiento de datos.

La Constitución Nacional, como Ley Suprema de la República, está obligada a garantizar derechos y garantías básicas, siendo el derecho a la intimidad, uno de ellos y, a tales efectos, se pronuncia en los términos del artículo 33 y, cuando esa intimidad tan celosamente puesta a salvo, incluso de la autoridad pública, está siendo agredida o en peligro de serlo por medio de la Informática, se impone un estudio pormenorizado de la cuestión y una reglamentación precisa de la norma constitucional.

[2] Op. Cit.; págs. 65-66.

[3] La *información* está compuesta por *documentación*, siendo ésta, el conjunto de datos, noticias, pruebas o antecedentes ciertos que se refieren a determinados asuntos y la información entendida como esa misma documentación, estructurada en función a determinados fines.

La protección jurídica de datos personales es la protección jurídica de las personas en lo que respecta al tratamiento automatizado de sus datos personales. El objeto de la protección no se circunscribe exclusivamente a los datos íntimos, sino a cualquier dato personal, pudiendo extenderse hasta los datos de carácter público, en lo que podría definirse como el amparo debido a la persona, contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, confeccionando una información identificable con ella, que afecte su entorno personal, social o profesional, dentro de los límites legales de la intimidad y es por esta circunstancia que, como mandato constitucional, surge la Ley Nº 1682, del 16 de enero de 2001, Que reglamenta la información de carácter privado, a efectos de tutelar el derecho a la intimidad de las personas. Dicha Ley vio modificado su contenido, con la promulgación de la Ley Nº 1969, el 2 de setiembre de 2002[4].

El derecho fundamental de las personas, en lo que respecta a la protección de los datos de carácter personal radica en la posibilidad de permitirle controlar sus datos, evitar el tráfico, poder disponer de ellos.

En la medida que estos valores no se vean alterados, la vigencia de la modernización seguirá justificándose, de lo contrario, si humanismo y tecnología transitan por vías separadas, el progreso sería una cáscara vacía sin valor ni sentido.

La última reunión que, sobre el tema, se celebró en el continente, arrojó los siguientes resultados en lo que respecta al Paraguay[5]:

> 1) El nivel de protección que ofrece la legislación nacional –Ley Nº 1682/2001 y Ley Nº 1969/2002- es insuficiente, a efectos de que Paraguay se acredite como nación *"adecuada"* ante los organismos de la Unión Europea.

[4] La Ley Nº 1969/2002, modificó los artículos 1º, 2º, 5º, 7º, 9º y 10 de la Ley Nº 1682/2001.
[5] Seminario Regional sobre Protección de Datos celebrado en el Centro de Formación de la AECID de Montevideo en junio de 2010.

2) *"Adecuación"* se traduce en términos económicos. La inversión europea es infinitamente superior en países *"adecuados"*, con relación a los países que no lo son.

3) *"Adecuación"* implica, en el caso paraguayo, una reforma a la legislación incluyendo distintas categorías de datos personales y la regulación necesaria para las transferencias internacionales de información; además, es imprescindible contar con un organismo administrativo que vele por el cumplimiento de las disposiciones legales.

4) La protección a la privacidad, es un factor de peso a la hora de mostrar el interés que tiene el país en el tema. No considerar este factor constituye una terrible afrenta a los Derechos Humanos y una nota negativa en cuanto a la consideración general del Paraguay como terreno fértil para inversiones.

5) En todo momento, la idea que debe prevalecer es la del no quebrantamiento del equilibrio que debe existir entre *"acceso a la información"* (Ley Nº 1728/2001) y *"privacidad"* (Ley Nº 1682/2001 y Ley Nº 1969/2002).

Esta obra pretende constituir un aporte hacia esa necesaria *"adecuación"*, denotando la trascendencia del tema en momentos en los que el Paraguay comienza a pisar fuerte y a marcar presencia dentro de la Sociedad de la Información

1.- LEGISLACIÓN

CONSTITUCIÓN NACIONAL

ARTICULO 33 - DEL DERECHO A LA INTIMIDAD

La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública.

Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas.

ARTICULO 135 - DEL HABEAS DATA

Toda persona puede acceder a la información y a los datos que sobre si misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.

LEY Nº 1682

DEL 16 DE ENERO DE 2001, QUE REGLAMENTA LA INFORMACIÓN DE CARÁCTER PRIVADO

EL CONGRESO DE LA NACION PARAGUAYA SANCIONA CON FUERZA DE LEY

Artículo 1°.- Toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado.

Artículo 2°.- Las fuentes públicas de información son libres para todos. Toda persona tiene derecho al acceso a los datos que se encuentren asentados en los registros públicos, incluso los creados por la Ley N° 879 del 2 de diciembre de 1981, la Ley N° 608 del 18 de julio de 1995, y sus modificaciones.

Artículo 3°.- Es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, que se realicen con fines científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudio de mercados, siempre que en las publicaciones no se individualicen las personas o entidades investigadas.

Artículo 4°.- Se prohíbe dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables.

Se consideran datos sensibles los referentes a pertenencias raciales o étnicas, preferencias políticas, estado individual de salud, convicciones religiosas, filosóficas o morales; intimidad sexual y, en general, los que fomenten prejuicios y discriminaciones, o afecten la dignidad, la privacidad, la intimidad doméstica y la imagen privada de personas o familias.

Artículo 5°.- Los datos de personas físicas o jurídicas individualizadas que revelen, describan o estimen su situación

patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales, podrán ser publicados o difundidos solamente:

a)Cuando esas personas hubiesen otorgado autorización expresa y por escrito para el efecto; y;

b) Cuando se trate de informaciones o calificaciones que entidades estatales o privadas deban publicar o dar a conocer en cumplimiento de disposiciones legales específicas.

Artículo 6°.- Podrán ser publicados y difundidos:

A) Los datos que consistan únicamente en nombre y apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional;

B) Cuando se trate de datos solicitados por el propio afectado; y,

C) Cuando la información sea recabada en el ejercicio de sus funciones, por magistrados judiciales, fiscales, comisiones parlamentarias o por otras autoridades legalmente facultadas para ese efecto.

Artículo 7°.- Serán actualizados permanentemente los datos personales sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales que de acuerdo con esta ley pueden difundirse o publicarse.

La obligación de actualizar dichos datos pesa sobre las empresas, personas o entidades que almacenan, procesan y difunden esa información. Las empresas, personas o entidades que utilizan sus servicios tienen la obligación de suministrarles la información pertinente a fin de que los datos que aquéllas almacenen, procesen y divulgue, se hallen permanentemente actualizados.

La actualización de los datos y el suministro de la información pertinente, deberán efectuarse dentro de los dos días hábiles siguientes al momento en que llegaren a su conocimiento por vía directa de la empresa o a través del afectado.

Artículo 8°.- Toda persona podrá acceder a la información y a los datos que sobre sí misma, sobre su cónyuge, sobre personas que acredite se hallen bajo su tutela o curatela, o sobre sus bienes, obren en registros oficiales o privados de carácter público o en entidades que suministren información sobre solvencia económica y situación patrimonial, así como conocer el uso que se haga de los mismos o su finalidad.

Artículo 9°.- Las personas, personas o entidades que suministran información sobre la situación patrimonial, la solvencia económica o sobre el cumplimiento de obligaciones comerciales no transmitirán ni divulgarán datos:

A) Sobre deudas vencidas no reclamadas judicialmente cuando la mora no sea superior a los noventa días;

B) Pasados cuatro años de la inscripción de deudas vencidas no reclamadas judicialmente, siempre que no consten nuevos incumplimientos del mismo deudor;

C) Pasados tres años del momento en que las obligaciones reclamadas judicialmente hayan sido canceladas por el deudor o extinguidas de modo legal;

D) Sobre deudas reclamadas en juicios en los que se haya producido la caducidad de la instancia o las demandas que fuesen rechazadas por los juzgados por sentencias firmes y ejecutoriadas, siempre que esos hechos hubieran llegado a su conocimiento por informaciones públicas o por los propios afectados;

E) Pasados cinco años del momento en que fueran suscriptas las inhibiciones generales de vender o gravar bienes, y, en el caso en que fueran reinscritas, después de los cinco años subsiguientes a esa reinscripción;

F) Pasados siete años de la fecha en que se haya dictado sentencia definitiva que determine obligaciones patrimoniales, en los que no conste su cumplimiento por el condenado;

G) Sobre sentencias declaratorias de quiebras después de siete años de su dictado, o, si se hubiese producido la

rehabilitación del fallido, después de tres años de ese hecho; y,

H) Sobre juicios de convocatoria de acreedores después de cinco años de la resolución judicial que la admita.

Las empresas o entidades que suministran información, sobre la situación patrimonial, la solvencia económica y el incumplimiento de compromisos comerciales deberán implementar mecanismos informáticos que de manera automática elimine de sus sistemas de información los datos no publicables, conforme se cumplan los plazos establecidos en este Artículo.

Artículo 10.- Se aplicarán las sanciones en los siguientes casos:

A) Las personas físicas o jurídicas que publiquen o distribuyan información sobre la situación patrimonial, solvencia económica o cumplimiento de obligaciones comerciales en violación de las disposiciones de esta ley serán sancionadas con multas que oscilarán, de acuerdo con las circunstancias del caso, entre trescientos y setecientos jornales mínimos para actividades laborales diversas no especificadas, multas que se duplicarán, triplicarán, cuadruplicarán, y así sucesivamente por cada reincidencia.

Para que se produzca la duplicación, triplicación, cuadruplicación, etc., se requerirá el previo reclamo del particular afectado.

B) Las personas físicas o jurídicas que, pese a estar obligadas a rectificar o a suministrar información para que se rectifiquen datos de acuerdo con lo que dispone el Artículo 7°, no lo hagan o lo hagan fuera de los plazos allí establecidos, serán sancionadas con multas que, de acuerdo con las circunstancias del caso, oscilarán entre ciento cincuenta y quinientos jornales mínimos para actividades laborales diversas no especificadas, multas que, en caso de reincidencia, serán aumentadas de acuerdo con la pauta establecida en el apartado a);

C) Si los reclamos extrajudiciales a los que se refiere el Artículo 8° no fueran atendidos sin razón o sin base legal, se aplicará a la entidad reacia al cumplimiento de sus obligaciones, una multa que, de acuerdo con las circunstancias del caso, oscilará entre cien y doscientos salarios mínimos para actividades laborales diversas no especificadas; y,

D) El juzgado ordenará que se efectúen las rectificaciones o supresiones que correspondan, y podrá ordenar también que la sentencia definitiva sea publicada en forma total, parcial o resumida, a costa del responsable.

Será competente para la aplicación de las multas el Juzgado en lo Civil y Comercial, en trámite sumario.

El cincuenta por ciento (50%) del importe total de las multas corresponderá al afectado, y lo restante será destinado a las instituciones correccionales de menores.

La aplicación de la multa no obstará a que la persona afectada promueva acción penal o acciones para reclamar la indemnización por daños y perjuicios.

Artículo 11.- La presente ley entrará en vigencia a los seis meses de su publicación, lapso en el cual las empresas, entidades y personas deberán adaptar a sus disposiciones, sus operaciones, registros, sistemas de información y de divulgación.

Artículo 12.- Comuníquese al Poder Ejecutivo.

Aprobado el Proyecto de Ley por la Honorable Cámara de Senadores de la Nación, el doce de diciembre del año dos mil y por la Honorable Cámara de Diputados, el veintiocho de diciembre del año dos mil, quedando sancionado el mismo, de conformidad con lo dispuesto en el Artículo 207, numeral 1) de la Constitución Nacional.

Juan Darío Monges Espínola
Vice-Presidente 1°
En Ejercicio de la Presidencia
H. Cámara de Diputados

Juan Roque Galeano Villalba
Presidente
H. Cámara de Senadores

Rosalino Andino Scavone
Secretario Parlamentario

Darío Antonio Franco Flores
Secretario Parlamentario

Asunción, 16 de enero de 2001

Téngase por Ley de la República, publíquese e insértese en el Registro Oficial.

El Presidente de la República

Luis Ángel González Macchi

Silvio Gustavo Ferreira Fernández
Ministro de Justicia y Trabajo

LEY Nº 1969

QUE MODIFICA, AMPLÍA Y DEROGA VARIOS ARTICULOS DE LA LEY N 1682/2001 "QUE REGLAMENTA LA INFORMACIÓN DE CARÁCTER PRIVADO"

EL CONGRESO DE LA NACION PARAGUAYA SANCIONA CON FUERZA DE

LEY

Artículo 1°.- Modifícanse los Artículos 1°, 2°, 5°, 7°, 9° y 10 de la Ley N° 1682/2001, cuyos textos quedan redactados de la siguiente manera:

> **"Art. 1°.-** Esta Ley tiene por objeto regular la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares. No se aplicará esta Ley en ningún caso a las bases de datos ni a las fuentes de informaciones periodísticas ni a las libertades de emitir opinión y de informar**".**
>
> **"Art. 2°.-** Toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado.
>
> Las fuentes públicas de información son libres para todos. Toda persona tiene derecho al acceso a los datos que se encuentren asentados en los registros públicos, incluso los creados por la Ley N° 879 del 2 de diciembre de 1981, la Ley N° 608 del 18 de julio de 1995, y sus modificaciones".

"Art. 5°.- Los datos de personas físicas o jurídicas que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales y financieras, podrán ser publicados o difundidos solamente:

A) cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente;

B) cuando se trate de informaciones o calificaciones que entidades estatales o privadas deban publicar o dar a conocer en cumplimiento de disposiciones legales específicas; y,

C) cuando consten en las fuentes públicas de información".

"Art. 7°.- Serán actualizados permanentemente los datos personales sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales y financieras que de acuerdo con esta Ley pueden difundirse.

La obligación de actualizar los datos mencionados en el párrafo anterior pesan sobre las empresas, personas o entidades que almacenan, procesan y difunden esa información. Esta actualización deberá realizarse dentro de los cuatro días siguientes del momento en que llegaren a su conocimiento. Las empresas, personas o entidades que utilizan sus servicios tienen la obligación de suministrar la información pertinente a fin de que los datos que aquéllas almacenen, procesen y divulguen, se hallen permanentemente actualizados, para cuyo efecto deberán comunicar dentro de los dos días, la actualización del crédito atrasado que ha generado la inclusión del deudor.

Los plazos citados precedentemente empezarán a correr a partir del reclamo realizado por parte del afectado.

En caso de que los datos personales fuesen erróneos, inexactos, equívocos o incompletos, y así se acredite, el afectado tendrá derecho a que se modifiquen.

La actualización, modificación o eliminación de los datos será absolutamente gratuita, debiendo proporcionarse además, a solicitud del afectado y sin costo alguno, copia auténtica del registro alterado en la parte pertinente".

Art. 9°.- Las empresas, personas o entidades que suministran información sobre la situación patrimonial, la solvencia económica o sobre el cumplimiento de obligaciones comerciales no transmitirán ni divulgarán datos:

B) pasados tres años de la inscripción de deudas vencidas no reclamadas judicialmente;

C) pasados tres años del momento en que las obligaciones reclamadas judicialmente hayan sido canceladas por el deudor o extinguidas de modo legal;

H) sobre juicios de convocatoria de acreedores después de cinco años de la resolución judicial que la admita.

Las empresas o entidades que suministran información sobre la situación patrimonial, la solvencia económica y el cumplimiento de compromisos comerciales y financieros deberán implementar mecanismos informáticos que de manera automática eliminen de su sistema de información los datos no publicables, conforme se cumplan los plazos establecidos en este Artículo".

"Art. 10.- Se aplicarán las sanciones en los siguientes casos:

A) las personas físicas o jurídicas que publiquen o distribuyan información sobre la situación patrimonial, solvencia económica o cumplimiento de obligaciones comerciales y financieras en violación de las disposiciones de esta Ley serán sancionadas con multas que oscilarán, de acuerdo con las circunstancias del caso, entre cincuenta y cien jornales mínimos para actividades laborales diversas no especificadas, multas que se

duplicarán, triplicarán, cuadruplicarán, y así sucesivamente por cada reincidencia del mismo afectado.

Para que se produzca la multa, la duplicación, triplicación, cuadruplicación, etc., se requerirá que la entidad reacia al cumplimiento de la actualización dentro del plazo establecido en el Artículo 7° de esta Ley, haya recibido el previo reclamo por escrito del particular afectado;

B) las personas físicas o jurídicas que, pese a estar obligadas a rectificar o a suministrar información para que se rectifiquen datos de acuerdo con lo que dispone el Artículo 7°, no lo hagan o lo hagan fuera de los plazos allí establecidos, serán sancionadas con multas que, de acuerdo con las circunstancias del caso, oscilarán entre cincuenta y cien jornales mínimos para actividades laborales diversas no especificadas; multas que, en caso de reincidencia, serán aumentadas de acuerdo con la pauta establecida en el apartado a).

Para que se produzca la multa, duplicación, triplicación, cuadruplicación, etc., se requerirá que la entidad reacia al cumplimiento de la actualización dentro del plazo establecido en el Artículo 7° de esta Ley, haya recibido el previo reclamo por escrito del particular afectado;

C) si los reclamos extrajudiciales a los que se refiere el Artículo 8° no fueran atendidos sin razón o sin base legal, se aplicará a la entidad reacia al cumplimiento de sus obligaciones, una multa que, de acuerdo con las circunstancias del caso, oscilará entre cien y doscientos jornales mínimos para actividades laborales diversas no especificadas;"

Artículo 2°.- Comuníquese al Poder Ejecutivo.

Aprobado el Proyecto de Ley por la Honorable Cámara de Diputados, a veintitrés días del mes de mayo del año dos mil dos, y por la Honorable Cámara de Senadores, a veintidós días del mes de agosto del año dos mil dos, quedando sancionado el mismo, de conformidad con lo dispuesto en el Artículo 207, numeral 2 de la

Constitución Nacional.

Oscar Alberto González Daré
Presidente
H. Cámara de Diputados

Raúl Antonio Ayala Diarte
Vicepresidente 1°
En ejercicio de la Presidencia
H. Cámara de Senadores

Juan José Vázquez Vázquez
Secretario Parlamentario

Ada Solalinde de Romero
Secretaria Parlamentaria

Asunción, 3 de setiembre de 2002.-

Téngase por Ley de la República, publíquese e insértese en el Registro Oficial.

El Presidente de la República
Luis Ángel González Macchi

Diego Abente Brun
Ministro de Justicia y Trabajo

REGLAS MÍNIMAS PARA LA DIFUSIÓN DE INFORMACIÓN JUDICIAL EN INTERNET
Reglas de Heredia

FINALIDAD

REGLA 1

La finalidad de la difusión en Internet de las sentencias y resoluciones judiciales será:

(a) El conocimiento de la información jurisprudencial y la garantía de igualdad ante la ley;
(b) Para procurar alcanzar la transparencia de la administración de justicia.

REGLA 2

La finalidad de la difusión en Internet de la información procesal será garantizar el inmediato acceso de las partes o quienes tengan un interés legítimo en la causa, a sus movimientos, citaciones o notificaciones.

DERECHO DE OPOSICIÓN DEL INTERESADO

REGLA 3

Se reconocerá al interesado el derecho a oponerse, previa petición y sin gastos, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de difusión, salvo cuando la legislación nacional disponga otra cosa. En caso de determinarse, de oficio o a petición de parte, que datos de personas físicas o jurídicas son ilegítimamente siendo difundidos, deberá ser efectuada la exclusión o rectificación correspondiente.

ADECUACIÓN AL FIN

REGLA 4

En cada caso los motores de búsqueda se ajustarán al alcance y finalidades con que se difunde la información judicial.

BALANCE ENTRE TRANSPARENCIA Y PRIVACIDAD

REGLA 5

Prevalecen los derechos de privacidad e intimidad, cuando se traten datos personales que se refieran a niños, niñas, adolescentes (menores) o incapaces; o asuntos familiares; o que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos; así como el tratamiento de los datos relativos a la salud o a la sexualidad; o victimas de violencia sexual o domestica; o cuando se trate de datos sensibles o de publicación restringida según cada legislación nacional aplicable o hayan sido así considerados en la jurisprudencia emanada de los órganos encargados de la tutela jurisdiccional de los derechos fundamentales.

En este caso se considera conveniente que los datos personales de las partes, coadyuvantes, adherentes, terceros y testigos intervinientes, sean suprimidos, anonimizados o inicializados, salvo que el interesado expresamente lo solicite y ello sea pertinente de acuerdo a la legislación.

REGLA 6

Prevalece la transparencia y el derecho de acceso a la información pública cuando la persona concernida ha alcanzado voluntariamente el carácter de publica y el proceso esté relacionado con las razones de su notoriedad. Sin embargo, se considerarán excluidas las cuestiones de familia o aquellas en los que exista una protección legal específica.

En estos casos podrán mantenerse los nombres de las partes en la difusión de la información judicial, pero se evitarán los domicilios u otros datos identificatorios.

REGLA 7

En todos los demás casos se buscará un equilibro que garantice

ambos derechos. Este equilibrio podrá instrumentarse:

(a) en las bases de datos de sentencias, utilizando motores de búsqueda capaces de ignorar nombres y datos personales;

(b) en las bases de datos de información procesal, utilizando como criterio de búsqueda e identificación el número único del caso.

Se evitará presentar esta información en forma de listas ordenadas por otro criterio que no sea el número de identificación del proceso o la resolución, o bien por un descriptor temático.

REGLA 8

El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública. Sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos.

REGLA 9

Los jueces cuando redacten sus sentencias u otras resoluciones y actuaciones, harán sus mejores esfuerzos para evitar mencionar hechos inconducentes o relativos a terceros, buscaran sólo mencionar aquellos hechos y datos personales estrictamente necesarios para los fundamentos de su decisión, tratando no invadir la esfera íntima de las personas mencionadas. Se exceptúa de la anterior regla la posibilidad de consignar algunos datos necesarios para fines meramente estadísticos, siempre que sean respetadas las reglas sobre privacidad contenidas en esta declaración. Igualmente se recomienda evitar los detalles que puedan perjudicar a personas jurídicas (morales) o dar excesivos detalles sobre los modus operandi que puedan incentivar algunos delitos. Esta regla se aplica en lo pertinente a los edictos judiciales.

REGLA 10

En la celebración de convenios con editoriales jurídicas deberán ser observadas las reglas precedentes.

DEFINICIONES

Datos personales: Los datos concernientes a una persona física o

moral, identificada o identificable, capaz de revelar información acerca de su personalidad, de sus relaciones afectivas, su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio físico y electrónico, número nacional de identificación de personas, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad o su autodeterminación informativa. Esta definición se interpretara en el contexto de la legislación local en la materia.

Motor de búsqueda: son las funciones de búsqueda incluidas en los sitios en Internet de los Poderes Judiciales que facilitan la ubicación y recuperación de todos los documento en la base de datos, que satisfacen las características lógicas definidas por el usuario, que pueden consistir en la inclusión o exclusión de determinadas palabras o familia de palabras; fechas; y tamaño de archivos, y todas sus posibles combinaciones con conectores booleanos.

Personas voluntariamente públicas: el concepto se refiere a funcionarios públicos (cargos electivos o jerárquicos) o particulares que se hayan involucrado voluntariamente en asuntos de interés público (en este caso se estima necesaria una manifestación clara de renuncia a una área determinada de su intimidad)

Anonimizar: Esto todo tratamiento de datos personales que implique que la información que se obtenga no pueda asociarse a persona determinada o determinable.

ALCANCES

Alcance 1. Estas reglas son recomendaciones que se limitan a la difusión en Internet o en cualquier otro formato electrónico de sentencias e información procesal. Por tanto no se refieren al acceso a documentos en las oficinas judiciales ni a las ediciones en papel.

Alcance 2. Son reglas mínimas en el sentido de la protección de los derechos de intimidad y privacidad; por tanto, las autoridades judiciales, o los particulares, las organizaciones o las empresas que difundan información judicial en Internet podrán utilizar procedimientos más rigurosos de protección.

Alcance 3. Si bien estas reglas están dirigidas a los sitios en Internet de los Poderes Judiciales también se hacen extensivas —en razón de la fuente de información— a los proveedores comerciales de jurisprudencia

o información judicial.

Alcance 4. Estas reglas no incluyen ningún procedimiento formal de adhesión personal ni institucional y su valor se limita a la autoridad de sus fundamentos y logros.

Alcance 5. Estas reglas pretenden ser hoy la mejor alternativa o punto de partida para lograr un equilibrio entre transparencia, acceso a la información pública y derechos de privacidad e intimidad. Su vigencia y autoridad en el futuro puede estar condicionada a nuevos desarrollos tecnológicos o a nuevos marcos regulatorios.

Heredia, 9 de julio de 2003.

Recomendaciones aprobadas durante el Seminario Internet y Sistema Judicial realizado en la ciudad de Heredia (Costa Rica), los días 8 y 9 de julio de 2003 con la participación de poderes judiciales, organizaciones de la sociedad civil y académicos de Argentina, Brasil, Canadá, Colombia, Costa Rica, Ecuador, El Salvador, México, República Dominicana y Uruguay.

ESTANDARES INTERNACIONALES SOBRE PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD

ESTANDARES INTERNACIONALES SOBRE PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD

RESOLUCIÓN DE MADRID[1]

Parte I
Disposiciones Generales

1 Objeto

El objeto del presente Documento es:

a. Definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal; y,

b. Facilitar los flujos internacionales de datos de carácter personal, necesarios para un mundo globalizado.

2 Definiciones

En el contexto del presente Documento, se entenderá por :

a. Dato de carácter personal: cualquier información concerniente a una persona física identifcada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados.

b. Tratamiento: cualquier operación o conjunto de operaciones, sean o no automatizadas, que se aplique a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión.

c. Interesado: persona física cuyos datos de carácter personal sean objeto de tratamietno.

1 Aprobada en la 31º Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en Madrid el 5 de noviembre de 2009.

d. Persona responsable: persona física o jurídica, de naturaleza pública o privada que, sola o en compañía de otros, decida sobre el tratamiento.

e. Prestador de servicios de tratamiento: persona física o jurídica, distinta de la persona rseponsable, que lleve a cabo un tratamiento de datos de carácter personal por cuenta de dicha persona responsable.

3 Ámbito de aplicación

1. El presente Documento está dirigido a su aplicación a todo tratamiento de datos de carácter personal, total o parcialmente automatizado, o realizado de forma estructurada en caso contrario, llevado a cabo tanto por el sector público como por el privado.

2. La legislación nacional aplicable podrá establecer que las disposiciones del presente Documento no sean aplicables al tratamiento de datos de carácter personal realizado por una persona física en el ejercicio de actividades relacionadas exclusivamente con su vida privada y familiar.

4 Medidas adicionales

1. Los Estados podrán completar el nivel de protección definido en el presente Documento con otras medidas adicionales que garanticen una mejor protección de la privacidad en relación con el tratamiento de datos de carácter personal.

2. Las disposiciones del presente Documento constituirán base apropiada para permitir las transferencias internacionales de datos de carácter personal, cuando éstas se realicen según lo indicado en el apartado 15 del presente Documento.

5 Excepciones

Los estados podrán limitar el alcance de las disposiciones recogidas en los apartados 7 a 10 y 16 a 18 del presente Documento cuando sea necesario, en una sociedad democrática, para preservar la seguridad nacional, la seguridad pública, la protección de la salud pública, o la protección de los derechos y las libertades de los

demás. Tales limitaciones deberán estar expresamente previstas por el derecho interno, de tal modo que se establezcan sus límites y se prevean las garantías adecuadas para preservar los derechos de los interesados.

Parte II
Principios básicos

6 Principio de lealtad y legalidad

1. Los tratamientos de datos de carácter personal se deberán realizar de manera leal, respetando la legislación nacional aplicable y los derechos y libertades de las persoanas, de conformidad con lo previsto en el presente Documento y con los fines y principios de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos.

2 En particular, se considerarán desleales aquellos tratamientos de datos de carácter personal que den lugar a una discriminación injusta o arbitraria contra los interesados.

7 Principio de finalidad

1. El tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas de la persona responsable.

2. La persona responsable se abstendrá de llevar a cabo tratamientos no compatibles con las finalidades para las que hubiese recabado los datos de carácter personal, a menos que cuente con el consentimiento inequívoco del interesado.

8 Principio de proporcionalidad

1. El tratamiento de datos de carácter personal deberá circunscribirse a aquéllos que resulten adecuados, relevantes y no excesivos en relación con las finalidades previstas en el apartado anterior.

2. En particular, la persona responsable deberá realizar esfuerzos razonables para limitar los datos de carácter personal tratados al mínimo necesario.

9 Principio de calidad

1. La persona responsable deberá asegurar en todo momento que los datos de carácter personal sean exactos, así como que se mantengan tan completos y actualizados como sea necesario para el cumplimiento de las finalidades para las que sean tratados.

2. La persona responsable deberá limitar el período de conservación de los datos de carácter personal tratados al mínimo necesario. De este modo, cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades que legitimaron su tratamiento, deberán ser cancelados o convertidos en anónimos.

10 Principio de transparencia

1. Toda persona responsable deberá contar con políticas transparentes en lo que a los tratamientos de datos de carácter personal que realice se refiere.

2. La persona responsable deberá facilitar a los interesados, al menos, información acerca de su identidad, de la finalidad para la que pretende realizar el tratamiento, de los destinatarios a los que prevé ceder los datos de carácter personal y del modo en que los interesados podrán ejercer los derechos previstos en el presente Documento, así como cualquier otra información necesaria para garantizar el tratamiento leal de dichos datos de carácter personal.

3. Cuando los datos de carácter personal hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en el momento de la recogida, salvo que se hubiera facilitado con anterioridad.

4. Cuando los datos de carácter personal no hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en un plazo prudencial de tiempo, si bien podrá sustituirse por medidas alternativas cuando su cumplimiento

resulte imposible o exija un esfuerzo desproporcionado a la persona responsable.

5. Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo, y ello en especial en aquellos tratamientos dirigidos específicamente a menores de edad.

6. Cuando los datos de carácter personal sean recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones establecidas en el presente apartado podrán satisfacerse mediante la publicación de políticas de privacidad fácilmente accesibles e identificables, que incluyan todos los extremos anteriormente previstos.

11 Principio de responsabilidad

La persona responsable deberá:

a. adoptar las medidas necesarias para cumplir con los principios y obligaciones establecidos en el presente Documento y en la legislación nacional aplicable, y

b. dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante las autoridades de supervisión en el ejercicio de sus competencias, conforme a lo establecido en el apartado 23.

Parte III
Legitimación para el tratamiento

12 Principio general de legitimación

1. Como regla general, los datos de carácter personal sólo podrán ser tratados cuando concurra alguno de los siguientes supuestos:

A. Previa obtención del consentimiento libre, inequívoco e informado del interesado.

B. Cuando un interés legítimo de la persona responsable justifique el tratamiento, siempre y cuando no prevalezcan los intereses legítimos, derechos o libertades de los interesados.

C. Cuando el tratamiento sea preciso para el mantenimiento o cumplimiento de una relación jurídica entre la persona responsable y el interesado.

D. Cuando el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable, o sea llevado a cabo por una Administración Pública que así lo precise para el legítimo ejercicio de sus competencias.

E. Cuando concurran situaciones excepcionales que pongan en peligro la vida, la salud o la seguridad del interesado o de otra persona.

2. La persona responsable deberá habilitar procedimientos sencillos, ágiles y eficaces que permitan a los interesados revocar su consentimiento en cualquier momento, y que no impliquen demoras o costes indebidos, ni ingreso alguno para la persona responsable.

13 Datos sensibles

1. Serán considerados sensibles aquellos datos de carácter personal:

A. Que afecten a la esfera más íntima del interesado; o

B. Cuya utilización indebida pueda:

i. Dar origen a una discriminación ilegal o arbitraria, o

ii. Conllevar un riesgo grave para el interesado.

2. En particular, serán considerados sensibles aquellos datos de carácter personal que puedan revelar aspectos como el origen racial o étnico, las opiniones políticas o las convicciones religiosas o filosóficas; así como los datos relativos a la salud o a la sexualidad. La legislación nacional aplicable podrá establecer otras categorías

de datos sensibles en caso de que ocurran las circunstancias a las que se refiere el párrafo anterior.

3. La legislación nacional aplicable deberá establecer las garantías necesarias para preservar los derechos de los interesados, que deberán fijar condiciones adicionales para el tratamiento de datos de carácter personal considerados sensibles.

14 Prestación de servicios de tratamiento

La persona responsable podrá realizar tratamientos de datos de carácter personal a través de uno o varios prestadores de servicios de tratamiento, debiendo para ello:

A. Velar porque cada prestador de servicios de tratamiento garantice, al menos, el nivel de protección previsto en el presente Documento y en la legislación nacional aplicable; y

B. Articular la relación jurídica a través de un contrato u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido, y que establezca el compromiso del prestador de servicios de tratamiento de cumplir con estas garantías y de asegurar que los datos de carácter personal sean tratados siguiendo las instrucciones de la persona responsable.

15 Transferencias internacionales

1. Como regla general, podrán realizarse transferencias internacionales de datos de carácter personal cuando el Estado al que se transfieran dichos datos ofrezca, cuando menos, el nivel de protección previsto en el presente Documento.

2. Será posible realizar transferencias internacionales de datos de carácter personal a Estados que no ofrezcan el nivel de protección previsto en el presente Documento, cuando quien pretenda transferir dichos datos garantice que el destinatario ofrecerá dicho nivel de protección; dicha garantía podrá derivarse, por ejemplo, de cláusulas contractuales apropiadas. En particular, cuando la transferencia se lleve a cabo en el seno de organizaciones

o grupos multinacionales, dicha garantía podrá consistir en la existencia de normas internas de privacidad cuya observancia resulte vinculante.

3. Asimismo, cuando sea necesario en el marco de una relación contractual en beneficio del interesado, o para proteger un interés vital del interesado o de otra persona, o para el cumplimiento de una obligación legal para la salvaguarda de un importante interés público, la legislación nacional aplicable a quien pretenda transferir datos de carácter personal podrá permitir la transferencia internacional de datos de carácter personal a Estados que no ofrezcan el nivel de protección previsto en el presente Documento.

4. La legislación nacional aplicable podrá atribuir a las autoridades de supervisión previstas en el apartado 23 la facultad de autorizar, con carácter previo a su realización, todas o algunas de las transferencias internacionales de datos de carácter personal originadas en su jurisdicción. En todo caso, quien pretenda realizar una transferencia internacional de datos de carácter personal deberá poder acreditar que la transferencia cumple las garantías establecidas en el presente Documento, y en particular cuando así le fuera requerido por las autoridades de supervisión en cumplimiento de las facultades previstas en el apartado 23.2.

Parte IV
Derechos del interesado

16 Derecho de acceso

1. El interesado tendrá derecho a recabar de la persona responsable, cuando así lo solicite, la información relativa a los concretos datos de carácter personal objeto de tratamiento, así como al origen de dichos datos, a las finalidades de los correspondientes tratamientos y a los destinatarios o las categorías de destinatarios a quienes se comuniquen o pretendan comunicar dichos datos.

2. Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo.

3. La legislación nacional aplicable podrá limitar el ejercicio reiterado de estos derechos, que obligaría a la persona responsable a responder múltiples solicitudes en intervalos cortos de tiempo, excepto en aquellos casos en los que el interesado haga constar en su solicitud un interés legítimo.

17 Derecho de rectificación y cancelación

1. El interesado tendrá derecho a solicitar a la persona responsable la rectificación o cancelación de los datos de carácter personal que pudieran resultar incompletos, inexactos, innecesarios o excesivos.

2. Cuando proceda, la persona responsable rectificará o cancelará los datos de carácter personal conforme a lo solicitado. Deberá, además, notificar este extremo a los terceros a quienes se hayan comunicado los datos de carácter personal, siempre que los mismos fueran conocidos.

3. La cancelación no procederá cuando los datos de carácter personal deban ser conservados para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable o, en su caso, por las relaciones contractuales entre la persona responsable y el interesado.

18 Derecho de oposición

1. El interesado podrá oponerse al tratamiento de sus datos de carácter personal cuando concurra una razón legítima derivada de su concreta situación personal.

2. No procederá el ejercicio de este derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable.

3. Cualquier interesado podrá oponerse, igualmente, a aquellas decisiones que conlleven efectos jurídicos basados únicamente en un tratamiento automatizado de datos de carácter

personal, excepto cuando la decisión hubiese sido expresamente solicitada por el interesado o sea precisa para el establecimiento, mantenimiento o cumplimiento de una relación jurídica entre la persona responsable y el propio interesado. En este último caso, el interesado debe tener la posibilidad de hacer valer su punto de vista, a fin de defender su derecho o interés.

19 Ejercicio de estos derechos

1. Los derechos previstos en los apartados 16 a 18 del presente Documento podrán ser ejercidos:

A. Directamente por el interesado, que deberá acreditar adecuadamente su identidad ante la persona responsable.

B. Por medio de representante, que deberá acreditar adecuadamente tal condición ante la persona responsable.

2. La persona responsable deberá implementar procedimientos que permitan a los interesados ejercer los derechos previstos en los apartados 16 a 18 del presente Documento de forma sencilla, ágil y eficaz, y que no conlleven demoras o costes indebidos, ni ingreso alguno para la persona responsable.

3. Cuando la persona responsable aprecie que, de acuerdo con la legislación nacional aplicable, no procede el ejercicio de los derechos previstos en la presente Parte, informará cumplidamente a interesado de los motivos que concurran en su apreciación.

Parte V
Seguridad

20 Derecho de oposición

1. Tanto la persona responsable como los prestadores de servicios de tratamiento deberán proteger los datos de carácter personal que sometan a tratamiento mediante aquellas medidas técnicas y organizativas que resulten idóneas en cada momento para garantizar su integridad, confidencialidad y disponibilidad. Tales medidas dependerán del riesgo existente, de sus posibles consecuencias para los interesados, del carácter especialmente

sensible de los datos de carácter personal, del estado de la técnica y del contexto en el que se efectúe el tratamiento, así como de las obligaciones establecidas en la legislación nacional aplicable.

2. Los interesados deberán ser informados por parte de quienes intervengan en cualquier fase del tratamiento de cualquier infracción de seguridad que pudiese afectar de forma significativa a sus derechos patrimoniales o extrapatrimoniales, así como de las medidas adoptadas para su resolución. Esta información deberá ser facilitada con antelación suficiente, para permitir la reacción de los interesados en defensa de sus derechos.

21 Deber de confidencialidad

La persona responsable y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal deberán respetar la confidencialidad de los mismos, obligación que subsistirá aún después de finalizar sus relaciones con el interesados o, en su caso, con la persona responsable.

Parte VI
Cumplimiento y supervisión

22 Medidas proactivas

Los Estados incentivarán, a través de su derecho interno, el establecimiento por quienes intervengan en cualquier fase del tratamiento de medidas que promuevan el mejor cumplimiento de la legislación que resulte aplicable en materia de protección de datos. Entre dichas medidas podrán encontrarse, entre otras:

A. El establecimiento de procedimientos destinados a prevenir y detectar infracciones, que podrán basarse en modelos estandarizados de gobierno y/o gestión de la seguridad de la información.

B.La designación, de uno o varios oficiales de privacidad o de protección de datos, con cualificación, recursos y competencias suficientes para ejercer adecuadamente sus funciones de supervisión.

C. La realización periódica de programas de concienciación, educación y formación entre los miembros de la organización destinados al mejor conocimiento de la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, así como de los procedimientos establecidos por la organización a tal efecto.

D. La realización periódica de auditorías transparentes por parte de sujetos cualificados y preferentemente independientes, que verifiquen el cumplimiento de la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, así como de los procedimientos establecidos por la organización a tal efecto.

E. La adaptación de aquellos sistemas y/o tecnologías de información destinados al tratamiento de datos de carácter personal a la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, en particular al decidir acerca de sus especificaciones técnicas y en su desarrollo e implementación.

F. La puesta en práctica de estudios de impacto sobre la privacidad previos a la implementación de nuevos sistemas y/o tecnologías de información destinados al tratamiento de datos de carácter personal, así como a la puesta en práctica de nuevas modalidades de tratamiento de datos de carácter personal o a la realización de modificaciones sustanciales en tratamientos ya existentes.

G. La adhesión a acuerdos de autorregulación cuya observancia resulte vinculante, que contengan elementos que permitan medir sus niveles de eficacia en cuanto al cumplimiento y grado de protección de los datos de carácter personal, y establezcan medidas efectivas en caso de cumplimiento.

H. La implementación de planes de contingencia que establezca unas pautas de actuación en caso de que se verifique un incumplimiento de la legislación que resulte

aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, y que incluya al menos la obligación de determinar la causa y alcance de la vulneración que se haya producido, de describir sus efectos negativos y de adoptar las medidas necesarias para evitar que se reproduzca en el futuro.

23 Supervisión

1. En cada Estado existirán una o más autoridades de supervisión que, de acuerdo con su derecho interno, serán responsables de supervisar la obsevancia de los principios establecidos en el presente Documento.

2. Dichas autoridades de supervisión deberán ser imparciales e independientes, y contarán con la cualificación técnica, las competencias suficientes y los recursos adecuados para conocer de las reclamaciones que le sean dirigidas por los interesados, y para realizar las investigaciones e intervenciones que resulten necesarias para garantizar el cumplimiento de la legislación nacional aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal.

3. En todo caso, y sin perjuicio de los recursos administrativos ante las citadas autoridades de supervisión, incluyendo el control jurisdiccional de sus decisiones, el interesado podrá acudir directamente a la vía jurisdiccional para hacer valer sus derechos conforme a las previsiones establecidas en la legislación nacional aplicable.

24 Cooperación y coordinación

1. Las autoridades de supervisión previstas en el apartado anterior procurarán cooperar entre sí en aras a una más uniforme protección de la privacidad en relación con el tratamiento de datos de carácter personal, tanto a nivel nacional como internacional. A los efectos de facilitar esta cooperación, los Estados deberán estar en disposición en todo momento de identificar las autoridades de supervisión competentes en su territorio.

2. Dichas autoridades realizarán, particularmente, los mayores esfuerzos para:

A. Compartir estudios, técnicas de investigación, estrategias comunicativas y de regulación y demás información que resulte de utilidad para el más eficaz ejercicio de sus funciones, en especial tras recibir una petición de apoyo por parte de otra autoridad de supervisión en el marco de una investigación o intervención;

B. Realizar investigaciones o intervenciones coordinadas, tanto a nivel nacional como internacional, en asuntos en los que concurra el interés de dos o más autoridades de supervisión;

C. Participar en asociaciones, grupos de trabajo y foros conjuntos, así como en seminarios, talleres o cursos que contribuyan a adoptar posturas comunes o a mejorar la cualificación técnica del personal que preste sus servicios a dichas autoridades de supervisión;

D. Mantener los niveles apropiados de confidencialidad con respecto a la información intercambiada en el curso de esta cooperación.

3. Los Estados impulsarán la creación de convenios de colaboración entre autoridades de supervisión, tanto regionales como nacionales o internacionales, que contribuyan a una más eficaz observancia del presente apartado.

25 Responsabilidad

1. La persona responsable será responsable de aquellos daños y/o perjuicios, tanto morales como materiales, que hubiesen causado a los interesados como consecuencia de un tratamiento de datos de carácter personal que hubiese vulnerado la legislación aplicable en materia de protección de datos, a menos que pueda demostrar que el daño no le puede ser atribuido. Ello, sin perjuicio de cualquier acción que la persona responsable pueda ejercer contra los prestadores de servicios de tratamiento que intervengan en cualquier fase del tratamiento.

2. Los Estados promoverán las medidas adecuadas para facilitar el acceso de los interesados a los correspondientes procesos judiciales o administrativos, que les permitan obtener la reparación de daños y/o perjuicios anteriormente mencionados.

3. La responsabilidad prevista en los párrafos anteriores existirá sin perjuicio de las sanciones penales, civiles o administrativas previstas, en su caso, por violación de la legislación nacional aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal.

4. La adopción de medidas proactivas como las previstas en el apartado 22 del presente Documento será tenida en cuenta al fijar la responsabilidad y las sanciones previstas en el presente apartado.

2.- DOCTRINA

LA PROTECCIÓN DE DATOS PERSONALES COMO NÚCLEO DEL DERECHO FUNDAMENTAL A LA AUTODERTERMINACIÓN INFORMATIVA. UNA MIRADA DESDE EL DERECHO ESPAÑOL Y EUROPEO

Adriana Raquel Marecos Gamarra[2]

INTRODUCCIÓN:

El presente trabajo tiene por objeto analizar el derecho fundamental a la autodeterminación informativa, el cual se ejerce a través de la protección de datos de carácter personal. Este es un derecho incluido por la doctrina en la tercera generación de derechos humanos, motivada por el reconocimiento de que en la actualidad los derechos humanos adquieren nuevos matices que responden al incipiente avance en la totalidad de las áreas de la vida en comunidad. Estos nuevos matices surgen para hacer frente a las necesidades de los individuos propias de la denominada era tecnológica y tienen como razón de ser un valor fundamental, la solidaridad.

Este estudio tiene su justificación en la relevancia que tiene este derecho fundamental en la actualidad, lo cual se evidencia a través de la preocupación que la sociedad está adquiriendo respecto a la protección de sus datos de carácter personal, como parte relevante de su dignidad. Hoy en día, más personas hacen uso del Internet y la cantidad de información que circula en la Red se duplica aceleradamente, lo cual ha llevado a la moderna sociedad de la información a convertirse en una verdadera "aldea global".

[2] Adriana Raquel Marecos Gamarra, es Abogada y Notaria Pública, egresada de la Facultad de Derecho y Ciencias Sociales de la Universidad Nacional de Asunción, es Máster en Protección de Derechos Humanos, por la Facultad de Derecho de la Universidad de Alcalá- España. Se desempeña como relatora de la Sala Constitucional de la Corte Suprema de Justicia y ejerce la docencia como titular de la cátedra de Derecho Constitucional II en la Facultad de Derecho, Ciencias Políticas y Sociales de la Universidad Americana y de las cátedras de Derechos Humanos y Derecho Internacional Público en la Facultad de Derecho y Ciencias Políticas de la Universidad del Norte.

El gran reto de la Nueva Era de la Información lo constituye la interconexión que es posible alcanzar con la ayuda de la moderna tecnología, muy especialmente a nivel de los ciudadanos y sus hogares. Este reto obliga a analizar los medios utilizados hasta ahora para proteger la autodeterminación informativa de los ciudadanos. Todo esto ha hecho que las pretensiones del desarrollo humano se amplíen y el individuo ya no solo aspira a ser protegido en su intimidad, sino que también pretende una calidad de vida en las relaciones y de apertura al mundo exterior, dando la posibilidad al individuo a que sea el mismo quien dirija y gobierne el ámbito y extensión de sus relaciones con terceros.

Los avances tecnológicos mencionados dieron lugar a las diferentes iniciativas que buscaron ampliar el alcance conceptual del derecho a la intimidad que provocó la construcción de un nuevo derecho, el derecho a la autodeterminación informativa, término que fue utilizado por primera vez en el año 1983 por el Tribunal Constitucional Alemán. A nivel europeo, en el marco del Consejo de Europa a través del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, se inicia el punto de partida del proceso de establecimiento del sistema regulador de protección de datos personales. Actualmente este texto se ve reforzado por una amplia regulación en esta materia, en especial a nivel comunitario por la Directiva 95/46/CE.

Este derecho, establecido en el artículo 18.4 de la Constitución Española no ha sido ajeno al Tribunal Constitucional Español, cuya doctrina configura el derecho a la protección de datos como un derecho fundamental autónomo. Este derecho fundamental no reduce su protección a los datos íntimos, sino que su objeto de protección es cualquier tipo de dato personal, traspasando su objeto la intimidad personal y viniendo constituido su contenido por un haz de facultades consistentes en diversos poderes que imponen a terceros, deberes tales como requerir el consentimiento para la recogida y uso de de los datos personales, ser informado sobre el destino y poder acceder, rectificar y cancelar los propios datos. En definitiva, el contenido del derecho a la protección de datos personales que reconoce el Tribunal incorpora

un poder de disposición y control sobre los datos personales, tanto frente al Estado como ante cualquier particular.

Si es evidente la consolidación del derecho a la autodeterminación informativa, no lo es menos su singularidad respecto a otras instituciones tradicionales, en tanto en cuanto ha sido fruto de unos parámetros sociales económicos, culturales y jurídicos muy determinados, que la hacen particularmente sensible a los continuos cambios que se suceden. Precisamente el presente trabajo, como habrá ocasión de incidir más adelante, pretende abundar en esta idea de institución moderna, producto de una época muy peculiar y sujeta, por ende, a la continua gestación y evolución que marcan los retos de la sociedad tecnológica.

El sistema jurídico español se encuentra a la vanguardia en lo que respecta a la protección de datos personales, teniendo en cuenta que este derecho se legisla ampliamente por la Ley 15/1999 Orgánica de Protección de Datos de Carácter Personal y cuenta también con las garantías necesarias de tal manera que el interesado, puede reclamar su derecho a la autodeterminación informativa a través de los mecanismos previstos para los derechos fundamentales como también a través de las garantías institucionales existentes.

La Agencia Española de Protección de Datos constituye una institución modelo a nivel europeo y es de notar su favorable evolución a lo largo de los años a partir de su creación. El trabajo que viene realizando la AEPD ha posibilitado a su vez un aumento de la conciencia de los individuos con respecto a la protección de sus datos personales en España, lo cual se evidencia a través del ejercicio de sus derechos por parte de los ciudadanos. Un claro ejemplo lo constituyen la creciente cantidad de consultas y denuncias que llegan diariamente a la AEPD, con lo cual se observa en los ciudadanos una notable preocupación por conocer como deben ejercitar mejor sus derechos.

Así mismo, se han dado a conocer las sanciones que ha impuesto la Agencia Española de Protección de Datos en el marco de la protección de este derecho fundamental, las cuales generan en la sociedad un mayor respeto del derecho a la protección de datos de carácter personal. Una de ellas fue confirmada por el

Tribunal Supremo, en la cual la Agencia impone al responsable en este caso a la productora del programa *Gran Hermano,* una sanción de 1,08 millones de euros, por el tratamiento dado a la información de carácter personal de unos 7.000 candidatos a participar en el espacio emitido por un canal de televisión, habiendo recabado datos sensibles relativos a la ideología, creencias religiosas, raza, salud y vida sexual sin que existiera consentimiento de los interesados, a fin de que estos datos se trataran informáticamente y cediendo los ficheros sin la debida seguridad a personas con las que no les unía ningún lazo contractual.

Es también importante agregar que este derecho encuentra singular importancia en el ámbito de los derechos humanos, teniendo en cuenta que como una consecuencia de los atentados terroristas del 11 de septiembre de 2001 acaecidos en los Estados Unidos y en respuesta a las presiones de la Administración norteamericana, el 16 de Diciembre de 2003 la Comisión Europea emitió un comunicado para el Consejo y el Parlamento Europeos, informando de las transferencias de datos de carácter personal, los llamados "*Passenger Name Record*" (PNR), que las autoridades aduaneras de los Estados Unidos exigían a las compañías aéreas europeas.

Estas transferencias se vienen realizando desde el mes de Marzo de 2004, de forma obligatoria, genérica, y bajo la amenaza de fuertes sanciones impuestas por la legislación estadounidense, a pesar de que éste, el país receptor, no cumplía las exigencias de "protección adecuada" de los datos de carácter personal que la normativa europea exige, lo cual ha generado una importante preocupación en el ámbito de la Unión Europea, teniendo en cuenta que con ello se estaría vulnerando no solamente la Directiva comunitaria, sino también las previsiones que sobre Derechos Fundamentales recogen documentos como la Convención Europea de Derechos Humanos (Viena, 1950) en su artículo 8, o la Carta de Derechos Fundamentales de la UE (2000) en sus artículos 7 y 8. La dificultad de enmarcar esta situación en la legalidad de la normativa europea, ha dado lugar a numerosos intercambios de información y negociaciones entre las autoridades

estadounidenses y las europeas, sin haber llegado aún a la solución de esta problemática.

Este trabajo se encuentra estructurado en cuatro capítulos en los cuales, se analiza primeramente la configuración jurídica del derecho a la autodeterminación informativa, con especial atención a su reconocimiento como derecho fundamental, en su segundo capítulo se aborda el estudio de la legislación específica de este derecho en España y Europa, que dan lugar al origen de los derechos que se reconocen a los individuos y los principios rectores del derecho a la protección de datos de carácter personal, los cuales son analizados con detenimiento en el tercer capítulo de este trabajo. Por último, se desarrollan en el cuarto capítulo, las garantías institucionales y jurisdiccionales previstas en el marco jurídico español y europeo a las que puede recurrir el interesado en la protección de sus datos de carácter personal.

Antes de concluir esta introducción es conveniente afrontar algunos extremos que, indudablemente, han de condicionar el contenido de las páginas posteriores. En lo que respecta al debate terminológico que se inclina ya sea por el término derecho a la protección de datos personales o derecho a la autodeterminación informativa, en el presente trabajo se utilizan ambos indistintamente como sinónimos por considerarse que éstos engloban igualmente el derecho objeto de desarrollo en las siguientes páginas.

CAPITULO I
CONFIGURACIÓN JURÍDICA DEL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA.

"Denominamos autodeterminación informativa a la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente los almacenados mediante medios informáticos."[3]

[3] L. E. VIGGIOLA y E. MOLINA QUIROGA, *Tutela de la autodeterminación informativa. Aproximación a una regulación eficaz del tratamiento de datos personales*. Ponencia presentada al Congreso Internacional "Derechos y Garantías en el Siglo XXI" de la Asociación de Abogados de Buenos Aires. Documento electrónico localizado en http://www.aaba.org.ar/bi151302.htm. Abril de 1999.

I. La Autodeterminación Informativa como Derecho de Tercera Generación:

Las relaciones humanas se encuentran en continua evolución, experimentando constantemente nuevos cambios, de acuerdo a este progreso, el derecho se adecua también a las diversas necesidades que surgen en la sociedad. Es así como deben ir siendo reconocidos los derechos fundamentales, siguiendo el ritmo evolutivo de las civilizaciones contemporáneas. Los derechos humanos son dinámicos, no se los puede concebir como categorías cerradas, sino que su reconocimiento debe ir ajustándose a fin de satisfacer las distintas necesidades que van surgiendo. Por lo expuesto anteriormente, se entiende que nuevos valores pueden ir incorporándose al catálogo de derechos fundamentales. De ésta manera también se podrían incluir normas que permitan responder a la necesidad de salvaguardar los derechos de las personas frente a las amenazas que vienen adheridas al avance de los medios informáticos y al progreso tecnológico.

Los derechos humanos devienen de ciertos valores ideológicos que surgen de acuerdo a un contexto histórico determinado. Así, encontramos a los derechos civiles y políticos o también llamados de primera generación, los cuales representan para el Estado una obligación de "no hacer", es decir, estos derechos se consideran suficientemente salvaguardados con el reconocimiento jurídico de una actitud pasiva por parte de los agentes del Estado y se refieren al derecho a la vida, a la intimidad, a la integridad física etc.[4]

Los movimientos reivindicativos evidenciaron la necesidad de completar el catálogo de los derechos y libertades de primera generación con una segunda generación de derechos, los llamados derechos económicos sociales y culturales, éstos alcanzan una paulatina consagración jurídica y política en la sustitución del

[4] Los derechos humanos de primera generación se encuentran reconocidos en el Pacto de Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966. Entrada en vigor: 23 de marzo de 1976, de conformidad con el artículo 49. Estos derechos pueden hacerse exigibles a través del Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 diciembre de 1966. Entrada en vigor: 23 de marzo de 1976, de conformidad con el artículo 9.

Estado liberal de derecho, por el Estado social de derecho. A diferencia de los derechos de primera generación, representan una obligación "de hacer" para el Estado, lo que conlleva a satisfacer las necesidades sociales de las personas, tales como el derecho a la salud, a la educación, etc., también denominados derechos de participación, con los cuales surge la obligación por parte del los poderes públicos de promover políticas sociales que permitan el acceso a estos servicios a toda la población.[5]

Finalmente llegamos a la tercera generación de derechos humanos, en la cual se incluyen nuevos derechos que surgen como respuesta al incipiente avance social. Como expone Pérez Luño[6], los derechos y libertades de la tercera generación se presentan como una respuesta al fenómeno de la denominada "contaminación de las libertades". La revolución tecnológica ha redimensionado las relaciones entre seres humanos y la de éstos a su vez con su entorno en el marco de su convivencia, e incidiendo estos cambios también en los derechos humanos que no quedan al margen de ello, viéndose afectados directamente.

Según Javier de Lucas[7], en lo que atañe al derecho a la autodeterminación informativa, el configurarlo como un derecho de tercera generación, fundamentado en la solidaridad, supone abandonar su concepción individualista derivada de su fuerte vinculación al derecho a la intimidad, ya que como afirma Pérez Luño[8], "la intimidad ha dejado de ser un privilegio del hombre aislado para devenir en un valor constitucional de la vida comunitaria"

Esta nueva generación contempla valores como la paz social, la calidad de vida, el derecho de los consumidores y el que especialmente interesa al presente trabajo, el derecho a la

[5] Los derechos de segunda generación se encuentran reconocidos en el Pacto Internacional de Derechos Económicos, Sociales y Culturales, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966.Entrada en vigor: 3 de enero de 1976, de conformidad con el artículo 27. Este Pacto no cuenta aún con Protocolo Facultativo.

[6] A. E. PÉREZ LUÑO, *La tercera generación de derechos humanos*. Aranzadi. Navarra. España 2006 p. 28

[7] J. DE LUCAS, *El concepto de solidaridad*, Fontamara, México 1993, p.19

[8] A.E. PÉREZ LUÑO, *Perfiles morales y políticos del derecho a la intimidad*, en Anales de la Real Academia de las Ciencias Morales y Políticas, año XLVIII, número 73, Madrid, 1996, p.319.

protección de las personas frente a las amenazas que vienen aparejadas del avance de las nuevas tecnologías y que da paso a un nuevo derecho, la autodeterminación en la esfera informativa. Estos nuevos derechos fundamentales ostentan una naturaleza jurídica propia, diferenciada de las anteriores generaciones de derechos fundamentales. Encontramos en la solidaridad la razón de ser de los derechos de tercera generación, como en su momento lo fue la libertad y la igualdad para los derechos de primera y segunda generación respectivamente. La solidaridad caracteriza a estos nuevos derechos ya que ellos se hallan aunados entre sí por su incidencia mundial en la vida de todos los hombres y exigen para su realización la comunidad de esfuerzos y responsabilidades a escala universal.

La característica esencial de los derechos de tercera generación es, para Vasak[9], que no pueden ser realizados más que con la conjunción de los esfuerzos de todos los actores del juego social: el individuo, el Estado, las entidades públicas y privadas, la comunidad internacional y su realización supone que exista un mínimo de consenso social a nivel nacional e internacional.

La nueva sociedad de la información, como se denomina el marco de convivencia en el que se desenvuelven los individuos en la actualidad, constituye un contexto en el cual nuestra vida individual y social corren riesgo de hallarse sometidas a lo que ha sido calificado por Frosini[10] como "*juicio universal permanente*", teniendo en cuenta que cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua e inadvertida, que potencialmente afecta incluso a los aspectos más sensibles de su vida privada.

Es posible afirmar que la etapa actual de desarrollo tecnológico, junto a avances y progresos indiscutibles, ha generado nuevos fenómenos de agresión a los derechos y libertades, con los avances de la informática el ser humano debe contar con las herramientas que le permitan reivindicar su derecho al desarrollo libre de su personalidad y a determinar como se llevará a cabo el

[9] K. VASAK, *Diferentes catégories des droits de I´homme*, en LAPEYRE, A., DE TINGUY, F. y VASAK, (Dir.): Les dimensions universelles des droits de I´homme, Bruylant, Bruxelles, 1990, p.303

[10] V. FROSINI, *Cibernética, derecho y sociedad*. Tecnos, Madrid, 1982 p.178

tratamiento de sus datos personales. Todo esto ha dado origen a una iniciativa tanto legislativa como jurisprudencial que tiende hacia el reconocimiento del derecho a la autodeterminación informativa como derecho fundamental. A fin de comprender como se ha llevado a cabo la consagración de este derecho fundamental, resulta necesario desarrollar y realizar un análisis de la evolución histórica del mismo.

Por otro lado, es posible encontrar percepciones distintas a las ya mencionadas, entre ellas se destaca la de Rodríguez Palop[11], quien considera al derecho a la autodeterminación informativa como un derecho asociado a la primera generación de derechos humanos, y afirma que éste cuenta con una doble dimensión, una individual o negativa, formulado como el derecho a la intimidad de la vida privada el cual parece aproximarse a los derechos de primera generación que tienen un carácter individualista y se inspiran en el valor de la libertad; en su dimensión social o positiva, en la medida en que exige una mayor participación de los ciudadanos, un control por parte de éstos de las tecnologías de la información y la comunicación , y una ampliación de sus posibilidades reales de intervenir en los procesos sociales y económicos en condiciones de igualdad, puede asemejarse a un derecho de participación política derivado de la libertad de informarse.

Si bien cabe afirmar que en el derecho a la autodeterminación informativa se vislumbran ciertos aspectos que también se encuentran en los derechos civiles y políticos, debe admitirse que este nuevo derecho fundamental cuenta con nuevas condiciones de ejercicio, derivadas del desarrollo que ha surgido en las sociedades tecnológicas, por lo tanto no es posible equipar completamente este derecho a los de la primera generación, no pudiendo ser por lo tanto incluido en esa categoría. Teniendo en cuenta lo expuesto, resulta necesario reconocer que en la actualidad, la consagración del derecho a la libertad informática y el derecho a la autodeterminación informativa *(Recht auf informationelle*

[11] M.E. RODRÍGUEZ PALOP, *La nueva generación de derechos humanos*, Dykinson, Madrid, 2002, p. 63

Selbsbestimmung)[12], en el marco de los derechos de la tercera generación, han determinado que se postule un status de *hábeas data*, concretando en las garantías de acceso y control a las informaciones procesadas en bancos de datos por parte de las personas concernidas e incluso ha avanzado hasta lograr no solo una protección jurisdiccional, sino también institucional, de este nuevo derecho fundamental.

Encontramos en los diferentes países europeos un aumento de la conciencia por la necesidad del reconocimiento de los derechos de tercera generación, y en especial por la protección de datos personales, corroborada por la creciente difusión de las instituciones de protección que tienden a completar la función de garantía de los tribunales. Entre algunas de esas instituciones podemos citar, al *Datainspektionen* en Suecia, al *Registertylsynet* en Dinamarca, al *Datatilsynet* de Noruega, a los *Datenschutzbeauftragten* en Alemania, al *College Bescherming Persoonsgegevens* en Holanda, al *Garante per la Protezione dei Dati Personali* en Italia, al *Commission Nationale de l'Informatique et des Libertés* en Francia y muy especialmente a la *Agencia Española de Protección de Datos* en España.

En definitiva y volviendo a las afirmaciones de Pérez Luño[13], la tercera generación de derechos humanos ha contribuido a redimensionar la nueva imagen del hombre en cuanto sujeto de derechos. Las nuevas condiciones de ejercicio de los derechos humanos han determinado una nueva forma de ser ciudadano en el Estado de Derecho de las sociedades tecnológicas, del mismo modo que el tránsito del Estado liberal al Estado Social de Derecho configuró también formas diferentes de ejercitar la ciudadanía.

II. Problemas terminológicos:

1. Relación y diferencias con otros términos análogos:

Privacidad, intimidad, imagen, honor, resumen el conjunto de valores implicados en la protección de datos, todos ellos objeto

[12] Denominación otorgada por el Tribunal Constitucional Alemán, en la sentencia que resuelve el recurso planteado contra la Ley del Censo en el año 1982.
[13] A. E. PÉREZ LUÑO, *La tercera generación de derechos humanos*. op. cit. p.35

de tutela a través de derechos fundamentales. Ciertamente estos derechos pueden verse vulnerados por la utilización abusiva de la tecnología informática, es por ello que se torna necesario realizar una acabada comparación de la figura del derecho a la autodeterminación informativa, con otros derechos similares, ya sea a fin de contrastar sus diferencias y poner de manifiesto también los aspectos que los relacionan, lo cual nos permitirá encuadrar y definir con mayor precisión el derecho objeto del presente estudio.

A. Derecho a la privacidad:

La privacidad, término castellanizado que proviene de la palabra anglosajona "*privacy*", constituye el conjunto de actividades que el hombre desarrolla en la colectividad y en grupos reducidos pero que desea preservar del conocimiento ajeno y, de su tratamiento informatizado, porque si bien podrían parecer informaciones inofensivas e intrascendentes para la persona afectada, la utilización y tratamiento informático de las mismas puede transformarla en comprometedoras para el libre desarrollo de la personalidad del individuo.

Encontramos los primeros esbozos de esta figura en el ensayo realizado en Estados Unidos por Warren y Brandeis en el año 1890, titulado "*The right to Privacy*" (el derecho a la privacidad), como una respuesta a las injerencias ilegítimas de la prensa en su vida privada, con él sentaron las bases técnico-jurídicas de la noción de privacidad, configurándola como el derecho a la soledad, como facultad "*to be alone*". [14]

Algunos conciben la "*privacy*" como la traducción de intimidad al idioma inglés, es así que en muchos textos relativos al estudio del derecho a la intimidad se citan a los autores Warren y Brandeis refiriéndose a su obra con el título "Derecho a la intimidad", lo cual ha generado confusiones a la hora del estudio y análisis del derecho a la privacidad. Pero la "*privacy*" en estos nuevos tiempos ya no puede ser concebida únicamente como un derecho asimilado al de la intimidad o "de estar solo", con el transcurso del tiempo ha ido adquiriendo un significado cautelar y

[14] S. WARREN y L. BRANDEIS, *The Right to Privacy*. Civitas. 1995 p. 22

preventivo, fundado en la idea de riesgo social que permite configurarlo como un derecho subjetivo autónomo llamado a tutelar la vida privada. La "*privacy*" en la actualidad se concibe por un sector doctrinal como una libertad positiva para ejercer un derecho de control sobre los datos referidos a la propia persona, y si estos han sido incorporados a un archivo electrónico, nada impide que puedan continuar bajo control y salvaguardia de su titular.

En definitiva, se identificaría con el mismo derecho a la autodeterminación informativa, porque ese es el significado de este derecho. Varios son los autores que opinan que el derecho a la privacidad constituye un sinónimo del derecho a la autodeterminación informativa, ya que a través de la protección de datos personales se busca justamente el disfrute de ese derecho a la privacidad el cual engloba la voluntad del individuo de determinar el fin para el cual se utilizarán sus datos y el tratamiento que se dará a los mismos.

Sin embargo, cabría hacer aquí una distinción, a la luz de la doctrina española, que establece la delimitación de los conceptos de privacidad y autodeterminación informativa, que define al primero como conjunto de aspectos de la vida de la persona que ésta desea y le es permitido mantener reservados, pese a no nacer de la esfera íntima, y el derecho a la autodeterminación informativa se identifica con las facultades, garantías y derechos que le son reconocidos a la persona para la adecuada protección frente al tratamiento automatizado de sus datos personales. Encontramos entonces que la privacidad constituye el bien de la persona digno de tutela, y el derecho a la autodeterminación informativa es la garantía que se establecen dentro del ordenamiento jurídico a fin de proteger ese bien.

B. Derecho a la intimidad:

Es necesario reconocer que el derecho a la autodeterminación informativa nace justamente con el fin de proteger el ámbito íntimo de la persona, sin embargo debe reconocerse la evolución conceptual que los separa y la especial naturaleza del bien jurídico y de los instrumentos de defensa que reconocen al individuo a través del derecho a la autodeterminación informativa y que no son

propios del derecho a la intimidad. La protección de datos no ha podido enmarcarse acabadamente en los instrumentos de tutela propios del derecho a la intimidad, ya que éste último es considerado dentro de un sistema meramente indemnizatorio, es decir, prevé medidas de naturaleza puramente represivas, lo cual resulta insuficiente teniendo en cuenta el fundamento del derecho a la autodeterminación informativa, que se caracteriza por contar tanto con medidas de carácter preventivo como sancionador.

Por lo tanto, y como bien lo aclara Garrido Gómez[15], "no estamos ante un garantismo (estatus negativo) de defensa frente a las intromisiones de la esfera privada que elude ser un derecho activo de control (estatus positivo) sobre el flujo de informaciones que conciernen a cada individuo".

Por lo tanto, el sistema jurídico de protección al que se acoge el derecho a la intimidad[16] no responde a los criterios fundamentales precautorios, que se observan en el objeto de la protección de datos personales, núcleo del derecho a la autodeterminación informativa. Teniendo en cuenta que la función del derecho a la intimidad es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad; y la protección de datos personales garantiza a esa persona un poder de control sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del afectado. De forma que mientras el primero faculta que se excluyan del conocimiento de los demás los datos de alguien, el segundo garantiza un poder de disposición[17].

[15] M. I. GARRIDO GÓMEZ, *Derechos fundamentales y Estado social y democrático de derecho*, Dilex, Madrid, 2007, p. 206

[16] La protección de este derecho se encuentra contemplada por la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen (BOE núm. 115, de 14-05-1982).

[17] L.J. MIERES MIERES, *Intimidad personal y familiar. Prontuario de jurisprudencia constitucional*, Editorial Aranzadi, S.A. Navarra 2002, p. 190-191 en M. I. GARRIDO GÓMEZ, *Derechos fundamentales y Estado social y democrático de derecho*, op.cit., p. 206

La creación tanto de garantías institucionales[18] como individuales constituyen un claro ejemplo de las medidas que requiere la protección de datos personales y que van más allá del marco normativo del derecho a la intimidad, aunque éste último se encuentra también protegido a través de estas medidas. Podemos concluir entonces que es posible lograr la protección del derecho a la intimidad a través de la protección de datos, más no es posible lograr acabadamente la protección de datos personales a través de las garantías de un derecho meramente negativo como el de la intimidad.

C. Derecho a la propia imagen:

Según Herrero-Tejedor, el derecho a la propia imagen nace históricamente unido a los derechos al honor y a la intimidad, como una mera manifestación de los mismos.[19] Encontramos también en la obra de Warren y Bradeis alusiones al derecho a la propia imagen, cuando hablaban del derecho de toda persona particular a impedir que su retrato circule sin su autorización, y del derecho de estar protegido de los retratos hechos a mano. [20]

Es posible afirmar que se identifica con otros derechos de libertad, y que se encuentra muy vinculado con el derecho a la intimidad, pero en la actualidad ha adquirido también autonomía y es considerado un derecho fundamental. El derecho a la propia imagen debe identificarse con los derechos de libertad, de manera que al individuo le es garantizado el derecho a decidir libremente respecto a su imagen, adoptando en su caso las medidas que procedan para impedir la divulgación de imágenes o retratos de la persona, aunque la misma no dañe su honor, ni interfiera en su derecho a la intimidad.[21]

[18] Entiéndase como garantías institucionales las instituciones administrativas de protección de datos que se encargan de tutelar los derechos de los ciudadanos, como ser la Agencia Española de Protección de Datos.
[19] F. HERRERO-TEJEDOR, *Honor, intimidad y propia imagen*. Colex. Madrid 1994 p. 22
[20] S. WARREN y L. BRANDEIS, *op. cit.*, p. 60
[21] Es también claro que no se requiere la intensión de dañar o de injuriar para que la libertad del sujeto, en cuanto a su imagen, se considere violada, y constituye una realidad incuestionable que el simple hecho de divulgar, exhibir o publicar la imagen de la persona puede y debe ser cuestión que quede al exclusivo arbitrio de cada persona.

La imagen de cada persona representa la reproducción del aspecto físico, constituye una manera de hacerse presente en la sociedad, ya que a través de la misma se manifiestan al exterior las cualidades propias del individuo y los aspectos integrantes de la personalidad del mismo.

Guarda gran relación con el derecho a la autodeterminación informativa, ya que la imagen constituye también un dato personal, pues permite identificar a una persona, por lo tanto también es objeto de tutela y debe ser salvaguardado a través de la protección de datos personales.

D. Derecho al honor:

El honor es considerado un valor íntimo del hombre, y forma parte de la personalidad del mismo, se encuentra conformado por la estima de los terceros sobre nuestra persona, así como por la consideración social, el buen nombre o fama junto al sentimiento y conciencia de la propia dignidad.

Desde el punto de vista jurídico, el derecho al honor constituye el derecho que cada ser humano tiene al reconocimiento de respeto, ante él mismo y ante las demás personas, de su dignidad humana y de los méritos y cualidades que ha ido adquiriendo como fruto de su desarrollo personal. La trascendencia del honor como bien de la persona se alcanza no sólo porque representa la expresión más esencial de la dignidad humana, sino porque presenta una dimensión social que supera el ámbito estrictamente individual.[22]

La distinción que cabe destacar entre el derecho al honor y el derecho a la autodeterminación informativa se encuentra en la propia norma protectora de estos derechos, mientras que las disposiciones que protegen el derecho al honor defienden al individuo frente a las divulgaciones inexactas o injuriosas de información relativa a su persona o a su familia, las normas de protección de datos tutelan cualquier tipo de dato personal, es decir, cualquier dato que permita identificar a una persona física, éstos no necesariamente deben tratarse de datos que puedan

[22] A. I. HERRÁN ORTIZ, *La violación de la intimidad en la protección de datos personales*. Dykinson. 1999. p. 38-39

afectar al honor de la persona. Sin embargo, es necesario acotar que ambos derechos son manifestaciones del más valioso bien que la persona humana posee, el respeto a su dignidad personal. La protección de datos personales es también un medio por el cual se puede llevar a cabo la defensa del honor.

III. La protección de datos personales como derecho fundamental autónomo:

¿Es el derecho a la autodeterminación informativa un derecho autónomo?

Es conveniente delimitar primeramente el derecho que será objeto de este estudio, así como también el proceso que dio paso a su génesis. El primer antecedente europeo de reconocimiento de la existencia del derecho a la autodeterminación informativa como un derecho autónomo, lo encontramos en la sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983, sobre la Ley del Censo de la población (Volkszählungsgesetzt) de 31 de marzo de 1982, en la cual éste tuvo la iniciativa en denominar de esta manera a este derecho, perfilándolo con mayor precisión y reconociendo a los ciudadanos el derecho a ser protegidos en lo que respecta al tratamiento automatizado de sus datos personales.

El recurso contra dicha Ley fue interpuesto por simpatizantes del movimiento de "los verdes", quienes obtuvieron una resolución cautelar del Tribunal Constitucional el 13 de abril de 1983, por la que se suspendió la entrada en vigor de la Ley del Censo y posteriormente la decisión definitiva sobre el fondo del recurso. En esta sentencia el Tribunal Constitucional germano señala que la proliferación de centros de datos ha permitido, gracias a los avances tecnológicos producir *"una imagen total y pormenorizada de la persona respectiva -un perfil de la personalidad-, incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en "hombre de cristal".*[23]

Precisamente, habiendo sido recurrida la legalidad de la Ley de Censo, por estimarse que la entidad y el número de preguntas

[23] M. DARANAS PELÁEZ (Trad.) *Jurisprudencia constitucional extranjera. Tribunal Constitucional Alemán.* Ley del Censo, BJC, núm. 33, 1984.

que él contenía importaba una lesión a la libertad personal, en Tribunal Constitucional Alemán estimó que: *"...el derecho general de la personalidad... abarca... la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida...: la libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona" y que... "... este derecho a la autodeterminación informativa no está, sin embargo, garantizado sin límites... el individuo tiene pues que aceptar en principio determinadas limitaciones de su derecho a la autodeterminación informativa en aras del interés preponderante de la comunidad".*[24]

Existen también autores que aportan ideas interesantes al respecto, como Erhard Denninger, quien manifiesta que el derecho a la autodeterminación informativa no ha surgido de la Sentencia mencionada más arriba, sino que deviene de un informe encargado por el Ministerio Federal del Interior, Steinmüller define sus estructuras fundamentales, introduciendo en aquella ocasión denominaciones como la del "derecho a la autodeterminación informativa sobre la imagen de una persona o grupo de personas" o el "derecho de autodeterminación del ciudadano referente a la imagen de su propia persona".[25]

En el ámbito español, a finales del los años setenta se inicia progresivamente una labor legislativa encaminada a garantizar el derecho de los ciudadanos, frente a las infinitas posibilidades de actuación que ofrece el medio informático respecto al tratamiento de la información personal, encontrándose ya el en el artículo 18.4 de la Constitución Española de 1978 un claro ejemplo de esa voluntad legislativa. Más adelante, en el siguiente capítulo del presente trabajo analizaremos con mayor detenimiento la normativa española en materia de protección de datos personales.

[24] P. LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa.* Tecnos. Madrid. 1990. p. 121-122.
[25] A. I. HERRÁN ORTIZ, *La violación de la intimidad en la protección de datos personales.* Dykinson. 1999.p. 73

1. Argumentación doctrinal:

No ha sido una cuestión pacífica la necesidad y oportunidad jurídica del reconocimiento de un nuevo derecho fundamental a la protección de datos personales, en efecto, fueron frecuentes e intensos los debates que enfrentaron a la doctrina a propósito de la configuración de este derecho. Dispares son las opiniones de los autores con respecto a ello y no han faltado opiniones críticas en la doctrina española, negando cualquier significación jurídica al derecho a la autodeterminación informativa, incluso rechazando la posibilidad de que el citado derecho goce de una existencia independiente y propia.

Se pueden distinguir dos sectores enfrentados, uno de los cuales rechaza la consideración del derecho a la autodeterminación informativa como derecho fundamental, argumentando que una reformulación del derecho a la intimidad es suficiente para ofrecer garantías individuales adecuadas; el otro sector sostiene, por el contrario, la idea de la necesidad ineludible de admitir la existencia de un nuevo derecho fundamental, cuya construcción se asienta sobre el reconocimiento al individuo de unas facultades de disposición y decisión respecto a sus propios datos personales, las cuales, a juicio de tales autores no sería posible deducir del tradicional derecho a la intimidad.

Garriga Domínguez defiende la autonomía del derecho a la autodeterminación informativa, argumentado la existencia de cruciales diferencias entre este derecho y el derecho a la intimidad, así afirma que éste último se trata de un derecho ligado a la dignidad humana, caracterizado por un eminente contenido negativo para salvaguardar del conocimiento ajeno una parte de nuestra vida – la más cercana – personal y familiar. El derecho a la autodeterminación informativa tiene un objeto y un contenido diferente, su ámbito es más amplio y los elementos que lo componen más complejos.

El tratamiento de la información personal puede, pero no tiene porque, afectar a informaciones íntimas o secretas que son objeto de protección del derecho a la intimidad, de la misma forma, los datos personales informatizados no tienen necesariamente que precipitar un retrato personal que implique una valoración

peyorativa u ofensiva de un individuo y que atente contra su buen nombre o fama.[26]

Una posición distinta es la defendida por Ruiz Miguel, quien considera que el derecho a la autodeterminación informativa no sería un nuevo derecho, sino que se trataría de "del mismo derecho a la intimidad auxiliado de nuevas técnicas y aplicado a un objeto nuevo, la informática". [27]

Lucas Murillo de la Cueva realiza un aporte interesante en el marco de este debate, aclarando que el bien que tutelan los sistemas de protección de datos no es la intimidad "física" o entendida en sentido estricto, sino la intimidad informativa o autodeterminación informativa, según este autor no caben dudas razonables que impidan hablar de la existencia de este nuevo derecho el cual se diferencia del derecho a la intimidad.[28]

El mismo autor se plantea la siguiente interrogante: ¿Cabe fundamentar el en el artículo 18.4 de la Constitución un derecho fundamental a la autodeterminación informativa? A ello responde que a su entender no puede ser otra que la afirmación de un derecho fundamental a la autodeterminación informativa; el bien jurídico a salvaguardar mediante este derecho es independiente, aunque en último extremo apunte a la preservación de la dignidad, identidad, y libertad de las personas, sin embargo, esa contribución la lleva a cabo por una vía propia. Es fácil comprobar que existe una defensa especial que pretende la satisfacción de un bien o interés dotado de entidad propia y justificación material suficiente.[29]

Entre otros argumentos que contribuyen a confirmar la necesidad de reconocer la existencia de un nuevo derecho fundamental a la autodeterminación informativa, se pueden citar la especialidad del bien jurídico objeto de protección, la caracterización de los derechos fundamentales como derechos dinámicos, acomodados a los cambios sociales y la exigencia de

[26]A. GARRIGA DOMÍNGUEZ. *Tratamiento de datos personales y derechos fundamentales*. Dykinson. Madrid. 2004. p.22

[27] C. RUIZ MIGUEL, *En torno a la protección de los datos personales automatizados*. Revista de Estudios Políticos (Nueva Época), num. 84 abril – junio. 1994 p. 241y 242.

[28] P. LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa*. Madrid. Tecnos. 1990. p 123.

[29] P. LUCAS MURILLO DE LA CUEVA, op. cit., p. 15

arbitrar nuevas formas de protección y garantías eficaces que aseguren al individuo un amparo adecuado de sus derechos y libertades frente a la invasión tecnológica.

Para Pérez Luño, la reticencia a reconocer la autodeterminación informativa como un derecho fundamental autónomo obedece, en otras ocasiones, al temor a que con ello se consagre una especie de derecho a la propiedad privada sobre los datos personales. Esta sería la actitud de Spiros Simitis, para quien la admisión de un derecho fundamental a la protección de datos o a la autodeterminación informativa favorecería, de facto, una concepción privatista de estos derechos. Se correría de este modo, el riesgo de concebirlos como derechos patrimoniales y de hipotecar su interpretación desde esa óptica "propietaria", que, además, se hallaría abocada a limitarlos por su conflicto con otros derechos fundamentales igualmente tutelados.[30]

Si bien la inquietud declarada por Simitis es pasible de ser compartida, pues el derecho a la autodeterminación informativa no debería de ser asumido como patrimonial, ya que ello implicaría desconocer su incuestionable dimensión social y comunitaria, este derecho representa un presupuesto básico para las formas de convivencia de las sociedades democráticas y pluralistas, al ser condición indispensable para el equilibrio de poderes y la participación activa de los ciudadanos en la vida pública, sin embargo, no por ello es necesario, que a fin de lograr dicho objetivo, sea sacrificada la autonomía de la autodeterminación informativa como derecho fundamental, para quedar relegada a mero apéndice de otros derechos básicos como el derecho a la intimidad. Debe interpretarse como el reconocimiento y garantía de un haz de facultades individuales que permiten al afectado un control y seguimiento de la información que registrada en soportes informáticos le concierne.

Siguiendo las afirmaciones de Pérez Luño, coincidimos en que el derecho a la autodeterminación informativa debe ser considerado como la respuesta del presente fenómeno de

[30] A. PÉREZ LUÑO, *Los derechos humanos en la sociedad tecnológica*, en Losano M. y otros: Libertad informática y leyes de protección de datos, Centro de Estudios Constitucionales. Madrid. 1990. p. 156.

contaminación de las libertades que amenaza con invalidar los logros del progreso tecnológico en los Estados de Derecho con mayor desarrollo económico. La inclusión de la libertad informativa en el catálogo de los derechos fundamentales representa en la actualidad una necesidad frente al progresivo avance informático[31]. Este autor reconoce que en algunas formulaciones doctrinales se concibe al derecho a la autodeterminación informativa como una categoría más restrictiva, al entenderlo como un aspecto del libre desarrollo de la personalidad o como una faceta de la intimidad. Conviene en todo caso, advertir que ambas categorías se condicionan mutuamente y representan los dos aspectos de la misma realidad, en este caso, un derecho fundamental. [32] El derecho a la autodeterminación informativa no puede desconocer su carácter de derecho fundamental por la circunstancia innegable de que tutela y ampara en último extremo valores fundamentales y esenciales del hombre como la dignidad y el libre desarrollo de la personalidad humana.

Herrán Ortiz, aporta otro importante argumento que avala la conveniencia de considerar como derecho fundamental autónomo a la autodeterminación informativa; y es que a través de esta confirmación de la independencia del derecho se alcanza un reforzamiento en su efectividad y en sus garantías.[33] La autora menciona que en el ordenamiento español existen muchas razones que permiten manifestar la conveniencia de articular la defensa de los derechos de la persona frente a las nuevas tecnologías informáticas a través de la construcción de una figura jurídica nueva, de un derecho que acoja en su contenido, sin necesidad de complicadas elucubraciones jurídicas, garantías y facultades individuales que permitan una defensa idónea y adecuada frente a la especial amenaza que representa la informática y sus complejos sistemas de información.

El peligro que representa la recopilación masiva de información, la cual constituye una forma de encasillar al titular de la información en categorías preestablecidas lo cual significa

[31]A. E. PÉREZ LUÑO. *Nuevos derechos fundamentales de la era tecnológica: la libertad informática*, ADPEP. núm. 2., 1989.p. 194.
[32] A. E. PÉREZ LUÑO op. cit., p. 175
[33] A. I. HERRÁN ORTIZ, op. cit., p. 121-122.

categorizar a los individuos a través de información obtenida de forma indiscriminada, es un claro ejemplo del cual proviene la necesidad de reconocer el derecho del ciudadano de tutelar sus datos personales. Otros peligros nacen cuando los datos se relacionan o conectan con otros datos de la persona, permitiendo acceder cada con mayor proximidad a la personalidad del individuo, utilizándose la información en la toma de decisiones sin tener en cuenta las peculiaridades de cada persona. Este tratamiento insensible de datos personales puede también ser utilizado con fines de control del individuo, cohibiéndole en el libre desarrollo de su personalidad al sentirse observado o vigilado y ocasionando que éste no actúe libremente, sino condicionado por lo que cree que se espera de él.

El reconocimiento del derecho fundamental a la autodeterminación informativa permite una mayor efectividad garantista, ya que si nos limitamos solo a tratar de salvaguardar los derechos de los ciudadanos a proteger sus datos personales con las herramientas jurídicas que devienen del derecho a la intimidad, no estaremos amparando el aspecto preventivo característico del derecho a la autodeterminación informativa, el cual no se contempla en la defensa del derecho a la intimidad, que más bien tiene un alcance meramente indemnizatorio para la víctima del agravio. Es necesario proveer al individuo de facultades que van más allá del la simple búsqueda del resarcimiento económico, otorgarles también instrumentos de actuación que les permitan a los titulares controlar y determinar el destino u otros aspectos del tratamiento de sus datos personales.

Este nuevo derecho, debe ser reconocido como un derecho fundamental autónomo, justamente, para lograr un mayor desarrollo legislativo y a través de ello generar por medio de la regulación correspondiente, los mecanismos que otorguen las suficientes garantías a los individuos, y sirva esto para tutelar intereses de la persona tales como la dignidad, la libertad personal o el desarrollo de la personalidad, fines que persiguen también otros derechos fundamentales ya reconocidos y que al guardar tan estrecha relación con el derecho a la autodeterminación informativa, no hacen más que confirmar la condición de derecho fundamental de éste último.

2. Argumentación jurisprudencial:

Numerosas y significativas han sido las ocasiones en que el Tribunal Constitucional Español se ha manifestado a propósito del reconocimiento del derecho a la autodeterminación informativa, si bien no es posible negar que, en sus primeros pronunciamientos se mostró vacilante. Así encontramos que por primera vez de pronunció sobre el alcance de esta garantía fundamental en la sentencia 254/1993, de 20 de julio, sentando desde ese momento las bases desde las que podemos iniciar la construcción del contenido esencial del derecho a la autodeterminación informativa. Sin embargo cabe destacar que el Tribunal Constitucional en dicho fallo prefiere el término "libertad informática".

Por medio de la sentencia recién mencionada podemos inferir que el Tribunal Constitucional no duda al afirmar que el artículo 18.4 de la Carta Magna española consagra un derecho fundamental autónomo y diferente del derecho a la intimidad, ya que en la misma, refiriéndose al artículo citado, manifiesta lo siguiente: *"… De este modo nuestra constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática…".*[34]

Si bien esta es la tesis general de la doctrina del Tribunal Constitucional Español, se halla una excepción en la Sentencia 143/1994, en la misma, asocia directamente la protección de los datos personales con el derecho a la intimidad, al que le reconoce un elemento positivo afirmando cuanto sigue *"…no es posible aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión…. En*

[34] STC 254/1993, de 20 de julio, fundamento jurídico 6, Recurso de Amparo Nº 1827/1990.

consecuencia con ello, habría que convenir en que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta."[35]

Vislumbramos mayor claridad en un fallo trascendental para la materia que estamos tratando; la sentencia 292/2000 de 30 de noviembre, que resolvió recurso de inconstitucionalidad núm. 1463-2000, interpuesto por el Defensor del Pueblo, contra los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En el mencionado fallo el Tribunal Constitucional realiza una clara y marcada diferenciación entre los conceptos de intimidad y protección de datos personales argumentando que *" La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran…la función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, 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."* [36]

En definitiva, a juicio del Tribunal Constitucional puede decirse que si el derecho a la intimidad aspira a garantizar al individuo un ámbito de reserva, y excluirlo del conocimiento ajeno, el derecho a la autodeterminación informativa reconoce a la persona un poder de control sobre la información personal que le

[35] STC 143/1994, de 09 de mayo, fundamento jurídico 7, Recurso de Amparo Nº 3192/1992.
[36] STC 292/2000, de 30 de noviembre, fundamento jurídico 5, Recurso de inconstitucionalidad Nº 1463-2000.

concierne, sobre su utilización y destino, para así evitar utilizaciones ilícitas.

Es importante agregar a lo ya mencionado, que el derecho fundamental a la intimidad no aporta por sí solo una protección suficiente a la nueva realidad derivada del progreso tecnológico y por ello, con la inclusión del apartado cuarto del artículo 18, se da respuesta a *"una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona"*[37]: la libertad informática.

Resumiendo, podemos afirmar, como también lo manifiesta Ana Garriga Domínguez, que el derecho a la autodeterminación informativa en el Derecho español se configura como un derecho fundamental autónomo e independiente del derecho a la intimidad, cuya finalidad, objeto y contenido difieren, habida cuenta de los distintos riesgos que ambos derechos fundamentales han de enfrentar en las sociedades actuales y conocemos los riesgos, sabemos que el derecho a la autodeterminación informativa se caracteriza por un marcado contenido positivo de control de los propios datos[38], pero ¿cuáles son los instrumentos que otorgan las facultades al ciudadano a fin de hacer efectivo su derecho a la autodeterminación informativa?¿cual es el contenido esencial del derecho fundamental previsto en el artículo 18.4 de la Constitución Española?¿cuáles son los derechos que le otorga al ciudadano la ley que desarrolla el artículo constitucional más arriba citado? Estas y otras interrogantes serán abordadas para su análisis y desarrollo en el siguiente capítulo del presente trabajo.

IV. Breve síntesis del desarrollo legislativo del derecho a la autodeterminación informativa:

Antes de adentrarnos en próximo capítulo en el cual se llevará a cabo el análisis de la regulación específica del derecho a la autodeterminación informativa en España y Europa, es menester primeramente conocer los orígenes y la evolución histórica de la legislación sobre protección de datos a nivel general. Varios autores dividen el estudio normativo de esta materia en leyes de

[37] STC 143/1994, de 09 de mayo, fundamento jurídico 6, Recurso de Amparo Nº 3192/1992
[38] A. GARRIGA DOMÍNGUEZ, op. cit., p. 36.

primera, segunda y tercera generación a fin de analizar la evolución legislativa en esta área del derecho.

1. Leyes de primera generación (1970-1973):

A lo largo de la primera mitad de la década de 1970 fueron aprobadas distintas normas de rango legal que la doctrina ha venido a denominar "leyes de primera generación", dada la escasez de desarrollo que la informática había tenido hasta aquellos momentos, pues se limitaba a crear instrumentos de protección y a fijar una limitación a la utilización desenfrenada de aquélla.[39]

En este marco, al *Land de Hesse* le corresponde el honor de haber adoptado la primera norma vinculante en materia de protección de datos, el 7 de octubre de 1970. La ley se refiere exclusivamente a ficheros de los organismos públicos y crea la figura del Comisario Parlamentario de Protección de Datos, con funciones similares a las de un *Ombudsman*, que velaba por el cumplimiento de la Ley y que entre otras funciones tenía la obligación de resolver los recursos que puedan promover aquellos interesados que consideren lesionados en sus derechos e intereses por el tratamiento de sus datos personales[40].

Por su parte, la primera Ley Nacional sobre protección de Datos fue aprobada por el Parlamento Sueco el 11 de mayo de 1973. Dicha Ley puede considerarse con propiedad el texto de referencia para el desarrollo posterior de la protección de datos de carácter personal, extendiendo su aplicación a la totalidad de los tratamientos del sector público y privado. Esta Ley desarrolla por primera vez los principios que configurar la protección de datos y crea la primera autoridad de protección de datos de carácter personal, el *Datainspektionen*.

[39] A. PUENTE ESCOBAR *Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal.* II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. 2ª Edición Protección de datos de carácter personal en Iberoamérica. Tirant lo Blanch.Valencia, 2006, p. 40

[40] A. GARRIGA DOMÍNGUEZ, *La protección de los datos personales en el derecho español,* Dykinson, Madrid, 1999. p. 48-49

2. Leyes de segunda generación (1974-1979):

Una nueva etapa en la evolución de las leyes de protección de datos se inicia con la promulgación de la *Privacy Act* estadounidense, de 31 de diciembre de 1974. El núcleo de esta ley reside en la protección de individuos frente al asalto a la intimidad[41] por los sistemas de acopio y almacenamiento de datos derivados del uso de la tecnología informática por las agencias federales, los bancos de datos de la administración federal[42]. Esta norma, se refería como la *Ley de Hesse* a ficheros de los Organismos Públicos. No obstante, la cuestión no fue objeto del desarrollo producido en Europa, es decir, a diferencia de los sistemas europeos, carece de una magistratura o institución especializada en vigilancia[43] y control de la aplicación de este sector normativo, debiendo dirigir directamente sus quejas las personas concernidas a los tribunales ordinarios.

En esta fase de preocupación por asegurar el derecho al acceso de las personas a las informaciones que les conciernen, y mostrando especial atención por la calidad de los datos, se sitúa la Ley francesa de 6 de enero de de 1978 relativa a *la Informatique, aux fichiers et aux libertés.* Uno de los aspectos centrales de esta norma reside en definir los datos personales y también prevé un órgano específico y de estructura colegiada para velar por su aplicación y recibir quejas de las personas afectadas denominado *Commssion Nationales de I´ Informatique et des Libertés*.

Durante este periodo, entre 1977 y 1979, la República Federal de Alemania, Dinamarca, Austria y Luxemburgo adoptan leyes nacionales de protección de datos de carácter personal, guiadas por el marco omnicomprensivo contenido en la legislación sueca

[41] La protección ligada a la privacidad de las personas, también era objeto de preocupación en los Estados Unidos, no siendo ajena a tal preocupación la inquietud social producida por el caso Watergate.

[42] A. E. PÉREZ LUÑO, *Los derechos humanos en la sociedad tecnológica*, en Losano M. y otros: Libertad informática y leyes de protección de datos, Centro de Estudios Constitucionales, op. cit p. 147

[43] La falta de interés por crear una institución especializada, se dio posiblemente por el papel preponderante que presenta la libertad de expresión e información en relación con la protección de la intimidad de las personas en la legislación Estadounidense.

de 1973 y creando en la mayor parte de los supuestos, autoridades independientes de protección de datos de carácter personal[44].

En la misma órbita de inquietudes, y como afirma Pérez Luño[45], por llevar al derecho positivo a la garantía de las facultades que dimana de la libertad informática se inscriben las primeras consagraciones de este derecho fundamental en las Constituciones de Portugal en 1976 y de España en 1978. La Constitución portuguesa consagra su artículo 35 a regular la utilización de la informática, mientras que la Constitución Española lo hace en su artículo 18.4.

Al propio tiempo, el Parlamento Europeo aprueba en 1979 la Resolución de 8 de mayo sobre tutela de los derechos del individuo frente al creciente progreso técnico en el sector de la informática, primer documento en materia de protección de datos dentro de la que luego sería la Unión Europea.

3. Leyes de tercera generación (1980-2000):

La tercera generación de Leyes de protección de datos personales se inicia con el reconocimiento, a escala internacional, de las facultades jurídicas que dimanan de la libertad informática. La aprobación de dos textos esenciales para la compresión del contenido del derecho fundamental a la protección de datos de carácter personal, como son la Recomendación de la OCDE sobre circulación de internacional de datos personales para la protección de la intimidad en septiembre de 1980 y el Convenio 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de sus datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, dan lugar a la iniciación de un nuevo y prolongado período en el que un gran número de países adaptarán su legislación a los principios consagrados en ambos instrumentos.

En este contexto, debe recordarse la Recomendación 81/679/CEE, de la Comisión Europea, en la que se aplaude la

[44] A. PUENTE ESCOBAR op. cit. p. 41

[45] A. PÉREZ LUÑO, *Los derechos humanos en la sociedad tecnológica*, en Losano M. y otros: Libertad informática y leyes de protección de datos, Centro de Estudios Constitucionales, op. cit p. 148

aprobación del Convenio 108 del Consejo de Europa y se aboga por la normalización del régimen jurídico de la protección de datos en los Estados Miembros instando a los mismos a ratificar el mencionado Convenio. Otros instrumentos internacionales tienen esencialmente en cuenta la regulación de la protección de datos de carácter personal, tales como los Convenio Schengen de 19 de enero de 1990, Europol de 26 de julio de 1995 y Cooperación en Materia Aduanera y creación del Sistema de Información Aduanero de 23 de enero de 1998.

Por otro lado, el 14 de enero de 1990 se aprueba la Resolución 45/95 de la Asamblea General de Naciones Unidas, relativa a los principios rectores para la reglamentación de los ficheros computarizados de datos personales[46]. Al propio tiempo, en el ámbito de la Unión Europea, durante este periodo se gesta la adopción del texto de mayor relevancia en el marco de la protección de datos, se trata de la Directiva 95/46/CE, cuya incidencia normativa de protección de datos es continua y creciente, inclusive más allá de la propia Unión Europea.

Actualmente, en el ámbito europeo, el derecho a la protección de datos de carácter personal es reconocido como derecho fundamental por el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, aprobada por los Jefes de Estado y de Gobierno de la Unión, celebrada en Niza el 7 de diciembre de 2000. La Carta reconoce el derecho a la protección de datos como independiente del derecho a la intimidad, y explicita claramente el contenido del derecho estableciendo lo siguiente:

> *"1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*
>
> *2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*

[46] También conocida como "Directrices de Protección de Datos de las Naciones Unidas" cuya importancia es capital, aún no tratándose de un texto obligatorio para los Estados Miembros, al suponer su adopción la aprobación del primer texto en materia de protección de datos de ámbito mundial.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente."

CAPITULO II
REGULACIÓN ESPECÍFICA DEL DERECHO FUNDAMENTAL A LA AUTODETERMINACIÓN INFORMATIVA EN ESPAÑA Y EUROPA:

I. Constitución Española, Art. 18.4:

Antes de iniciar el estudio pormenorizado de la legislación vigente que desarrolla el artículo 18.4 de la Constitución Española de 1978, es conveniente primeramente, examinar los antecedentes que dieron origen a la norma constitucional que fuera la génesis de lo que posteriormente daría lugar a la nueva Ley Orgánica de Protección de Datos.

Los constituyentes españoles tomaron, en este caso, el ejemplo de la Constitución portuguesa de 1976, que sólo dos años antes a la española había incluido esta protección como precepto normativo y que fue una de las primeras en hacerse eco de la necesidad de dar carácter de derecho fundamental a la salvaguarda de los datos personales frente al uso de la informática.

Según comenta Lucas Murillo de la Cueva[47], la única modificación significativa realizada al artículo 18. 4 previsto en el anteproyecto se dio durante los debates que tuvieron lugar en la Comisión de Asuntos Constitucionales y Libertades Públicas del Congreso de Diputados. La discusión de una enmienda de la Minoría Catalana y de otra del Señor Sancho Rof, del Grupo Parlamentario de UCD, dieron lugar a una serie de intervenciones que condujeron, tras las correspondientes votaciones, a la redacción definitiva del precepto. El señor Sancho Rof abogaba, con su enmienda 716, por la supresión del último párrafo del actual artículo 18.4, ya que entendía que no añadía nada al reconocimiento general del apartado primero a favor del derecho a la propia imagen. Por otro lado el representante de la Minoría

[47] P. LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa*. Tecnos. 1990.p. 150-152

Catalana, señor Roca Junyent defendió su postura señalando lo siguiente:

> *"[…] cuando la Ponencia limita este uso [de la informática] a los daños que puedan producirse al honor, a la intimidad personal y familiar, se queda simplemente enana reflexión parcial de los problemas, porque lo realmente grave aparece cuando esta información que puede dañar al honor incide en el ejercicio de los derechos por parte de los ciudadanos, es decir, cuando un ciudadano, por ejemplo, deseando constituir una asociación o promocionar una reunión, o bien practicar una actividad económica, encuentra que , por razón de una información de la que el no él no es conocedor y respecto de la cual no puede incluso no pronunciarse en muchas ocasiones, se limita de tal manera el ejercicio de sus derechos que se ve colocado en una situación de inferioridad y desigualdad frente a los ciudadanos. […] Por ésta razón nosotros insistimos en nuestra enmienda que fundamentalmente supone incorporar entre los límites de la informática el de que se garantice el pleno ejercicio de los derechos por parte de los ciudadanos".*

Las intervenciones que se produjeron y las que provocaron la enmienda número 117 de Minoría Catalana llevaron a la mayoría de la Comisión a ratificar la fórmula inicial de la ponencia, si bien ampliando el ámbito material, incorporándose con ella entre los límites de la informática, el de que se garantice el pleno ejercicio de los derechos por parte de todos los ciudadanos.[48]

Otro aspecto digno de destacar, es la duda que genera el artículo 18.4, en lo que respecta a los titulares del derecho a la autodeterminación informativa, ya que la mencionada norma, establece la garantía del pleno ejercicio de los derechos por parte de todos los ciudadanos, por lo tanto, esto daría pie a que se interpretara el artículo de tal manera que únicamente las personas de nacionalidad española gozarían de este derecho.

[48] Al aprobar la enmienda, ésta fue la redacción definitiva del artículo 18.4:
La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derecho

Como advierte Herrán Ortiz[49], pese a la indudable necesidad de extender la titularidad a cualquier persona física sea o no de nacionalidad española, resida o no en España, no se acierta a comprender el desliz del artículo 18.4 de la Constitución al indicar que *"la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los* ***ciudadanos*** *y el pleno ejercicio de sus derechos"*. No sólo incomprensible, sino además injustificada resulta la limitación constitucional en la condición de sujeto activo del derecho a la autodeterminación informativa. Si el propio artículo 18 de la Constitución reconoce la titularidad de los derechos al honor, a la intimidad personal y familiar y a la propia imagen, a la inviolabilidad del domicilio o al secreto de las telecomunicaciones a cualquier persona, no se comprende qué ha movido al legislador constitucional a limitar la titularidad del derecho a la autodeterminación informativa y restringirla a los ciudadanos.

Por otro lado, también resultará contradictorio concebir el derecho a la autodeterminación informativa como derecho de los ciudadanos en particular y no como derecho fundamental reconocido a toda persona física, independientemente de su condición de ciudadano, especialmente si se atiende a lo dispuesto en el artículo 13 de la Constitución Española que al regular los derechos de quienes no disfrutan la nacionalidad española dispone que: *"Los extranjeros gozarán en España de las libertades públicas que garantiza el presente Título en los términos que establezcan los Tratados y la Ley"*. Entre las libertades públicas que se garantizan en el Título I, destaca la limitación en el uso de la informática que, por lo tanto, ha de garantizarse de forma equivalente para toda persona independientemente de su nacionalidad.

II. Las Directrices de la OCDE (Organización para la Cooperación y el Desarrollo Económico):

Es importante considerar el trabajo realizado desde la OCDE[50] en materia de protección de datos, destacando dos

[49] A. I. HERRÁN ORTÍZ, *La violación de la intimidad en la protección de datos personales.* Dykinson. Madrid. 1999. p. 234-235

[50] Resulta importante destacar que el principal motivo que llevó a la OCDE a elaborar una normativa sobre el tratamiento de datos personales fue la preocupación que algunos países,

Recomendaciones publicadas desde este organismo: La Recomendación sobre "circulación internacional de datos personales para la protección de la intimidad" y la Recomendación relativa a la "seguridad de los sistemas de información".

Estas Directrices constituyen documentos orientativos de la actividad de los Estados miembros de esta organización, sin perjuicio de la recomendación que los mismos contienen de cumplir los principios establecidos en esos textos. Arenas Ramiro[51], al realizar el análisis de este tema, manifiesta acertadamente que estos documentos no son jurídicamente vinculantes, sino más bien meras disposiciones mínimas que recomiendan a los Estados seguir una serie de principios generales en materia de tratamiento de datos personales, no obstante, tienen por objeto el establecimiento de una regulación básica de protección de datos que garantice el libre flujo de la información entre los Estados participantes en los mismos.

Primeramente cabe analizar la recomendación de la OCDE sobre circulación internacional de datos personales para la protección de la intimidad, la cual fue adoptada el 23 de septiembre de 1980 y constituye el primer documento de ámbito supranacional que analiza en profundidad el derecho a la protección de datos de carácter personal.

La Recomendación se estructura en cinco partes diferenciadas, la primera parte de carácter general, establece las definiciones aplicables a la Recomendación, incluyendo específicamente los conceptos de dato personales, responsable del tratamiento, afectado y transferencia internacional de datos. Además, establece determinadas declaraciones referidas a su ámbito de aplicación, a fin de que no pueda considerarse que el establecimiento de los estándares previsto en las directrices pueda implicar una reducción del respeto a la intimidad. Del mismo modo, se indica que las directrices son aplicables a los sectores público y privado y que las mismas constituyen un catálogo de

especialmente Estados Unidos, mostraban ante las iniciativas nacionales que iban surgiendo sobre protección de datos y el temor a que la regulación de esta materia creara barreras proteccionistas en el comercio internacional.

[51] M. ARENAS RAMIRO, *El derecho fundamental a la protección de datos personales en Europa*. Agencia Española de Protección de Datos. Tirant lo Blanch, Valencia, 2006 p. 160

mínimos en esta materia, al disponer el apartado 6 que las directrices *"deben ser consideradas un estándar mínimo y pueden ser complementadas por medidas adicionales de protección de la privacidad y las libertades individuales"*.

La segunda parte viene a establecer los principios básicos que han de regir el tratamiento de datos de carácter personal y que han de regir la regulación nacional que pudiera ser adoptada en esta materia. Estos principios, que como se dijo, constituyen el germen de todas las normas nacionales e internacionales adoptadas en materia de protección de datos con posterioridad, y pueden resumirse, como los identifica Agustín Puente Escobar[52], en los siete siguientes:

- Los datos deberán ser recogidos y tratados de forma leal y lícita, recabándose previamente el consentimiento del interesado, o al menos informando al mismo de esa recogida.
- El responsable del tratamiento deberá especificar la finalidad para la que trata los datos, no pudiendo utilizar los mismos para un fin incompatible con la finalidad declarada.
- Los datos sometidos a tratamiento deben ser adecuados, pertinentes y no excesivos en relación con la finalidad declarada.
- El responsable del tratamiento deberá adoptar las medidas de seguridad en el tratamiento, necesarias para evitar la pérdida o acceso no autorizado a los datos.
- El responsable del tratamiento deberá informar a los afectados acerca del tratamiento de sus datos de carácter personal que se proponga realizar.
- Los afectados tienen derecho a conocer la existencia de un tratamiento de sus datos de carácter personal.

[52]A. PUENTE ESCOBAR *Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal.* II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. 2ª Edición Protección de datos de carácter personal en Iberoamérica. Tirant lo Blanch.Valencia, 2006, p. 52

- Los afectados tienen derecho a solicitar, en su caso, la rectificación o cancelación de sus datos sometidos a tratamiento.

La tercera parte de la recomendación se centra en el estudio de las transferencias internacionales de datos de carácter personal, de forma que se garantice el libre flujo de los mismos. En este sentido, el apartado 16 exige a los Estados miembros garantizar la seguridad del tráfico de la información.

El requisito para que proceda la transferencia internacional de datos es que el Estado de destino "*observe sustancialmente las directrices*". Además, podrán establecerse restricciones adicionales en relación con ciertas categorías de datos para los que la Ley nacional establezca reglas especiales en atención a su naturaleza, si el Estado de destino no ofrece un nivel de protección equivalente.

Por último, los apartados cuarto y quinto regulan las medidas de implantación de las directrices y la cooperación entre los Estados miembros. En cuanto a las medidas de implantación de las directrices, se indica en el apartado 19 el deber de los Estados miembros de establecer medidas legales, administrativas de otra índole para la protección de la privacidad y las libertades individuales en relación con los datos personales. En particular, las directrices se refieren a la adopción de normas nacionales y al fomento de la autorregulación y la adopción de códigos de conducta. Sin embargo, debe destacarse que la Recomendación no hace en ningún momento referencia a la creación de autoridades nacionales de protección de datos personales, sino que únicamente impulsa la adopción de medidas nacionales de desarrollo de las directrices.

Estas Directrices se complementan con la adopción, el 26 de noviembre de 1992 de la Recomendación OCDE relativa a la seguridad de los sistemas de información, la cual se encuentra más enfocada hacia cuestiones económicas y legales relativas a las transmisiones internacionales de datos, telecomunicaciones y servicios.[53]

[53] M. ARENAS RAMIRO, op. cit, p.160

III. Convenio 108 del Consejo de Europa, de 1981 sobre el Tratamiento automatizado de datos de carácter personal:

1. Importancia y contenido:

Siguiendo las afirmaciones de Pérez Luño[54], la ratificación por parte de España, con fecha de 27 de enero de 1984 del Convenio 108 ha tenido una importante incidencia en el sistema jurídico Español. Esto se ve justificado constitucionalmente, ya que por imperio del artículo 96.1 de la CE de 1978, los Tratados internacionales válidamente celebrados, una vez publicados oficialmente en España, formarán parte del ordenamiento interno. Cumplidos ambos requisitos, el texto del Convenio Europeo, forma parte del sistema jurídico español, y hasta el año 1982, constituyó la norma básica en materia de protección de datos personales frente a los abusos cometidos en su procesamiento informático.

Como sustenta Heredero Higueras[55], la ratificación del Convenio 108 representó, sin duda alguna, un avance positivo en materia de protección de datos para el ordenamiento español, en tanto que facilitó la efectividad y aplicación plena del texto bajo los auspicios del Comité Consultivo, que ha cuidado y velado por la correcta aplicación de aquél a través de la formulación de propuestas y dictámenes, ya sea de oficio o a instancia de parte, si bien en España su aplicación se hallaba condicionada a la efectiva elaboración de una legislación que posibilitara la plena efectividad de las medidas protectoras, que en el citado Convenio se reconocían.

El texto del Convenio se halla integrado por un conciso Preámbulo y veintisiete artículos los cuales se agrupan en siete Capítulos. En el Preámbulo se reitera la finalidad prioritaria del Consejo de Europa cifrada en facilitar la unión entre sus miembros, que se funda en el respeto de la preeminencia del derecho y de los

[54] A. E. PÉREZ LUÑO, *Los derechos humanos en la sociedad tecnológica*, Cuadernos y Debates 21. Centro de Estudios Constitucionales. Bilbao. España 1989. p.163-164

[55] M. HEREDERO HIGUERAS, *La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*, en Jornadas sobre "Informática Judicial y Protección de Datos Personales", celebradas en San Sebastián el 7 y 8 de octubre de 1993, Departamento de Justicia del Gobierno Vasco, Victoria- Gasteiz, Servicio Central de Publicaciones, 1994, p.44

derechos humanos. Se indica también, de forma expresa, que el objeto inmediato del Convenio, reside en conciliar los valores básicos "del respeto a la vida privada y de la libre circulación de la información entre los pueblos".

En cuanto al objeto del Convenio 108[56], éste se refiere únicamente a la garantía del respeto a sus derechos y libertades fundamentales, por lo que no se trata tanto de limitar la utilización de la informática, como de "asegurar" y preservar el respeto de los derechos fundamentales de la persona, con especial consideración al derecho a la vida privada. Examinando el objeto de este instrumento internacional, en contraste con lo establecido en el artículo 18.4 CE, es posible afirmar que los mismo difieren, en cuanto que el texto constitucional proclama de manera explícita la limitación en el uso de la informática para garantizar los derechos y libertades fundamentales.[57]

Con respecto a la titularidad de derechos previstos en el Convenio, éste ha sido pensado para la protección de las personas físicas, según lo establece su artículo 2 inc. a), sin embargo, como comenta Pérez Luño[58], es posible, si así lo estipula un Estado parte, proyectar su normativa a la tutela de las personas jurídicas. Este autor considera que dicha posibilidad, no es irrelevante por la dificultad que plantea extender a las personas jurídicas categorías como las de vida privada o intimidad, que fueron concebidas en función de los intereses de las personas individuales.

El aspecto más destacable y relevante dentro del Convenio es su capítulo segundo en el que se indican los principios básicos para la protección de los datos personales, dentro del que se establece el principio de calidad, exigiendo que los mismos hayan de ser pertinentes, no excesivos y mantenerse actualizados.

---

[56] Esto queda estipulado por el artículo primero del Convenio que establece:
Artículo 1. Objeto y fin
El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal, correspondientes a dicha persona («protección de datos»).

[57] A. I. HERRÁN ORTÍZ, op. cit., p.195

[58] A. E. PÉREZ LUÑO, op. cit., p. 168

Así mismo, enuncia las categorías particulares de datos, como aquellos que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, condenas penales estableciendo que no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. También fija criterios para la información, consentimiento y ejercicio de derechos para los titulares de los datos. De igual modo, no olvida indicar la necesidad de establecer las medidas de seguridad necesarias, así como el desarrollo de las sanciones y los recursos necesarios por cada país.

Al margen de dicho capítulo en el que se establecen los puntos más relevantes del Convenio, el capítulo tercero trata sobre los flujos transfronterizos de datos hecho éste que refleja la preocupación existente al respecto ya que el Consejo siempre fue consiente del progresivo incremento del flujo de datos.

Desde el momento en que España ratifica el Convenio 108 del Consejo de Europa se compromete a adoptar medidas legislativas que sean necesarias para facilitar la correcta aplicación del Convenio, existiendo para ello un límite temporal, lo cual significa que a la fecha de entrada en vigor del Convenio las mismas han de estar aprobadas[59]. En el caso particular de España el legislador, luego de ratificar el Convenio, tardó ocho años en introducir una legislación interna en materia de protección de datos.

2. El Protocolo adicional del Convenio 108:

No obstante la enorme importancia del Convenio 108 en el establecimiento de una serie de principios de obligado cumplimiento en materia de protección de datos de carácter personal, el transcurso de 20 años desde su adopción y la irrupción de otros instrumentos posteriores, como la Directiva 95/46/CE, vinculante para todos los Estados miembros de la Unión Europea,

[59] Esto se encuentra establecido en el artículo 4 del Convenio, el cual dice:
Artículo 4. Compromisos de las Partes
1. Cada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.
2. Dichas medidas deberán adoptarse a más tardar en el momento de la entrada en vigor del presente Convenio con respecto a dicha Parte.

signatarios asimismo del Convenio 108, exigía la adaptación de algunas de las previsiones del Convenio al régimen existente tras la adopción de la Directiva.

Ello dio lugar a la adopción, el 8 de noviembre de 2001, de un Protocolo adicional del Convenio 108, que completa las previsiones del Convenio en determinadas materias, tales como los movimientos internacionales de datos y la exigibilidad de la existencia en los Estados signatarios de una autoridad independiente cuya función sea, precisamente, el velar por el cumplimiento de las disposiciones nacionales adoptadas en materia de protección de datos de carácter personal.

El Protocolo, en vigor desde la ratificación del mismo por Chipre (quinto país en ratificarlo), en marzo de 2004, tiene, en consecuencia, por objeto, subsanar las lagunas del Convenio 108 y garantizar su aplicación por los Estados Parte, perfeccionando asimismo el régimen de las transferencias internacionales de datos.

En cuanto a su articulado, el artículo primero dispone que cada Estado parte deberá crear una o varias autoridades independientes de protección de datos, que habrá de tener poderes de investigación, facultades para instar la adopción de resoluciones judiciales y poderes para resolver las reclamaciones de los ciudadanos.

En lo referente a las transferencias internacionales de datos, el artículo segundo del Protocolo dispone que *"cada parte preverá que la transferencia de datos personales a un destinatario sometido a la competencia de un Estado u organización que no es parte del Convenio se lleve a cabo únicamente si dicho Estado u organización asegura un adecuado nivel de protección"*. Dicha regla sólo se verá exceptuada si el derecho interno así lo establece a causa de los intereses concretos del afectado, o intereses legítimos, especialmente los de carácter público, o si se prevén las suficientes garantías, que pueden resultar, en particular, de cláusulas contractuales, por parte del responsable del tratamiento responsable de la transferencia y dichas garantías se estiman por las autoridades competentes de conformidad con el derecho interno.

IV. Ley Orgánica 5/1992 del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD):

Tras la incorporación constitucional en 1978 del derecho a la protección frente al uso informático de los datos personales, transcurrieron varios años[60], hasta que octubre de 1992 se dictó la Ley 5/1992, Orgánica del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD). Cuando las Cortes Generales deciden afrontar el desarrollo legislativo del artículo 18.4 del texto fundamental, utilizaron las experiencias de otros países y el derecho comparado sobre el tema, teniendo en cuenta principalmente las previsiones del Convenio 108 del Consejo de Europa, de 28 de enero de 1981, de protección de las personas con respecto al tratamiento automatizado de sus datos de carácter personal.[61]

La LORTAD incluye en su exposición de motivos una serie de aspectos en relación con los principios establecidos en ella que definen el espíritu seguido por el legislador. En cuanto al ámbito de aplicación, el legislador consideró conveniente la permanencia de ciertas leyes especiales que ya contienen regulación suficiente en relación a la protección de datos y que se refieren a ámbitos que revisten singularidad en cuanto a sus funciones, mecanismos de puesta al día y rectificación por lo que se aconsejó el mantenimiento de su régimen específico.

En la Ley 5/92 se realiza un análisis del concepto de intimidad, contrastándolo con el de privacidad, de este modo el legislador manifiesta textualmente que:

[60] Varios son los autores que consideran grave la tardía regulación interna del Convenio 108, por parte del Gobierno español, por cuanto que el propio preámbulo del Convenio pone acento en la intensificación tanto interna como internacional en el tratamiento informatizado de los datos personales, que hace precisa la ampliación de las garantías de los derechos y libertades fundamentales de la persona. Por lo tanto resulta incompresible que la promulgación de una ley protectora de los datos personales haya sido demorada, teniendo en cuenta que el texto ratificado por España, contenía afirmaciones tan clarificadoras respecto a la amenaza que para los valores fundamentales del hombre encierra la informática.

[61] Cabe resaltar que la consideración de ese documento internacional no permanecía a la discrecionalidad de las cámaras, sino que era exigida por la misma Constitución, ya que en su artículo 10.2 establece que las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce, se interpretarán de conformidad con la Declaración Universal de los Derechos Humanos, y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

> *"El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los* tres primeros párrafos del artículo 18 de la Constitución *y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo."*[62]

Un aspecto importante a destacar es el objeto que establecía la LORTAD, siendo éste la regulación de los ficheros automatizados sin tener en cuenta los ficheros manuales o en soporte papel, aspecto que ha variado en la normativa vigente.

Muchas han sido las críticas realizadas a la Ley 5/1992, entre ellas la gran inequidad existente entre el eficaz seguimiento que se efectuaba del tratamiento automatizado de los datos de carácter personal dentro del ámbito privado, mientras que en el caso de los ficheros de titularidad pública se establecía una serie de excepciones que provocaba la sensación para los titulares de los datos de una nula efectividad de la defensa de su intimidad, lo que dio pie a la presentación de recursos ante el Tribunal constitucional por parte del Defensor del Pueblo y del Partido Popular. También el Consejo Ejecutivo de la Generalitat de Cataluña presentó un recurso ante el mismo órgano por considerar que ésta norma no

[62] Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. (Vigente hasta el 14 de enero de 2000)

respetaba el marco de distribución competencial entre el Estado y las Comunidades Autónomas.

La Sentencia 290/2000, de 30 de noviembre, emanada del Tribunal Constitucional, resuelve los recursos mencionados, y tal como se indica en su texto, son objeto de la misma los artículos 6.2, 19.1, 20.3. 22.1, 22.2, 24, 31, 30.1, 30.2, 40.1, 40.2, y la Disposición Final Tercera de la Ley. Asimismo se recuerda que los recursos acumulados se refieren, en unos casos, a normas de carácter sustantivo, derogadas al tiempo de dictarse la LOPD, y, por otra, a normas que pudieran afectar la atribución de competencias entre el Estado y las Comunidades Autónomas. Por ello, la Sentencia analiza separadamente unas y otras.

En relación con las normas sustantivas, en su Fundamento Jurídico 3, recuerda que *"en aquellos casos en los que los preceptos objeto de un recurso de inconstitucionalidad fueron impugnados por motivos distintos de los referidos al orden de reparto competencial entre el Estado y las Comunidades Autónomas, la regla general es que su derogación al tiempo de resolver dicho recurso produce la extinción del mismo, por pérdida sobrevenida sobre su objeto. Con la reserva, claro es, de que un determinado precepto, pese a su derogación, pudiera continuar proyectando sus efectos sobre situaciones posteriores a ese momento si así se desprende con toda evidencia de los términos en los que tal derogación se ha producido por la ley posterior"*.

La Sentencia señala que procede estimar la pérdida sobrevenida de objeto en cuanto a los recursos de inconstitucionalidad fundados en aspectos sustantivos de la Ley. Del mismo modo el Tribunal resolvió no entrar en análisis de lo establecido en aquéllas normas de la LORTAD reproducidas por la nueva LOPD y que habían sido objeto de recurso por parte del Defensor del Pueblo, dado que las mismas serían analizadas, resolviéndose la constitucionalidad o inconstitucionalidad de las mismas en la Sentencia que recayera sobre el citado recurso.

Dicho esto, el Tribunal centra su análisis en el estudio de las normas referidas a la existencia o inexistencia de una infracción del reparto competencial establecido en la Constitución Española. Así, el Tribunal Constitucional razona que *"cabe apreciar, en primer*

lugar, una identidad sustancial de contenidos respecto al artículo 24 LORTAD y el que le ha sucedido en el tiempo (artículo 26 LOPD), salvo ciertas precisiones en su apartado 2. Y otro tanto cabe decir, en segundo término respecto a los artículo 31 y 40.1 y 2 LORTAD respecto de los correspondientes de la Ley posterior (artículos 32 y 41 LOPD), sin entrar a conocer del recurso interpuesto contra el artículo 39 de la LORTAD, por la novedad introducida en el artículo 40 de la LOPD, que sustituye la referencia a la Agencia de Protección de Datos por una referencia genérica a las autoridades de control". En consecuencia, la Sentencia analiza exclusivamente las tachas de inconstitucionalidad que, desde la perspectiva del orden constitucional de distribución de competencias entre el Estado y las Comunidades Autónomas, se han dirigido contra los artículos 24, 31 y 40.1 y 2 LORTAD.

En cuanto a este análisis, su fundamento jurídico 7 considera necesario *"que el examen de la presente disputa competencial se lleve a cabo partiendo de dos presupuestos, a saber: el contenido del derecho fundamental a la protección de datos personales y, en segundo término, los rasgos generales que caracterizan a la Agencia de Protección de Datos dado que la función de este órgano es la de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación",* como se expresaba en el primer inciso del apartado a) del artículo 36 LORTAD.

El análisis de la primera de las cuestiones, el Tribunal Constitucional recuerda que el derecho consagrado en el artículo 18.4 de la Constitución "*es, además, en sí mismo, un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama la informática*". Este derecho fundamental comprende, según indica el Tribunal un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos, de suerte que "*es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí*

considerado por parte de las Administraciones Públicas competentes".

Por otra parte, y en relación con la segunda de las cuestiones apuntadas, el fundamento jurídico 8 de la Sentencia señala que *"en lo que respecta a las funciones y potestades atribuidas a la Agencia de Protección de Datos, el apartado a) del artículo 36 LORTAD ofrece una caracterización general de las primeras al encomendar a la Agencia la función general de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial respecto a los derechos de información, acceso, rectificación y cancelación de datos"*. Y en cuanto a especificación de esta función de carácter tuitivo en orden a la protección de datos personales, *"los restantes apartados del citado precepto le atribuyeron tanto funciones de intervención o control respecto a ciertos sujetos y actividades como funciones registrables y consultivas"*.

Se alegaba por las Comunidades Autónomas *"que las actividades relativas a los ficheros automatizados de carácter personal no son en sí mismas el objeto de una materia competencial, sino que constituyen una actividad instrumental al servicio de otras actividades encuadrables dentro de otras materias sobre las que las Comunidades Autónomas pueden ostentar títulos competenciales según el orden constitucional de reparto de competencias"*. Sin embargo, el Tribunal Constitucional considera que tal argumento no resulta admisible por cuanto, con su planteamiento "se está desvirtuando cuál es el bien jurídico constitucionalmente relevante, que no se es otro que la protección de los datos de carácter personal frente a un tratamiento informático que pueda lesionar ciertos derechos fundamentales de los ciudadanos o afecta al pleno ejercicio de sus derechos, como claramente se desprende del temor de dicho precepto constitucional".

Por último, en su fundamento jurídico 14, la Sentencia recuerda que *"la exigencia constitucional de protección de los derechos fundamentales en todo el territorio nacional requiere que éstos, en correspondencia con la función que poseen en nuestro ordenamiento (artículo 10.1 CE), tengan una proyección directa sobre el reparto competencial entre el Estado y las Comunidades Autónomas para asegurar la igualdad de todos los españoles en su*

disfrute. Así mismo, que dicha exigencia faculta al Estado para adoptar garantías normativas y, en su caso, garantías institucionales".

"A ese fin -prosigue la Sentencia- la LORTAD ha atribuido a la Agencia de Protección de Datos diversas funciones y potestades, de información, inspección y sanción, para prevenir las violaciones de los derechos fundamentales antes mencionados. Y dado que la garantía de estos derechos, así como la relativa a la igualdad de todos los españoles en su disfrute es el objetivo que guía la actuación de la Agencia de Protección de Datos, es claro que la funciones y potestades de este órgano han de ejercerse cualquiera que sea el lugar del territorio nacional donde se encuentren los ficheros automatizados contenidos dados de carácter personal y sean quienes sean los responsables de tales ficheros".

En consecuencia, concluye la Sentencia, *"es la garantía de los derechos fundamentales exigida por la Constitución así como la de la igualdad de todos los españoles en su disfrute la que en el presente caso justifica que la Agencia de Protección de Datos puede ejercer las funciones y potestades a las que antes se ha hecho referencia respecto a los ficheros informatizados que contengan datos personales y sean de titularidad privada",* por lo que las normas discutidas son consideradas por el alto Tribunal como conformes a la Constitución".

Finalmente, el motivo que logró la redacción de una nueva norma y derogación de la LORTAD, fue la necesidad de adaptar la normativa española al contenido de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, éste texto indicaba un plazo de transposición de tres años, alargándose en algunos puntos muy concretos hasta 12 años.[63]

[63] Y. NAVALPOTRO NAVALPOTRO, VV.AA. *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, Valladolid, 2005. p.42-43

V. La Directiva 95/46/CE y su transposición al derecho español:

Según comenta Herrán Ortiz,[64] desde el ámbito comunitario siempre se ha mostrado especial sensibilidad por conciliar la protección de datos con la libre circulación de datos personales, y así, esta preocupación se ha manifestado en la Directiva 95/46/CE que en su artículo 1.2 previene que *"los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en el apartado 1"*. Por ello, la Directiva no se presenta como un texto restrictivo para la circulación de los datos personales en el ámbito comunitario, antes bien, al contrario, como el propio título de la Directiva revela, el verdadero espíritu que animó la elaboración del texto comunitario no fue otro que servir de instrumento para el libre flujo de datos personales en la Unión Europea.

En consecuencia, los Estados pueden establecer un reforzamiento en los mecanismos de protección de los derechos de las personas frente al tratamiento de datos, si bien este fortalecimiento nunca podrá implicar un obstáculo al libre flujo de información en el marco comunitario, ya que tal y como explícitamente previene la Directiva en la Exposición de Motivos "*el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros*".

La Directiva 95/46/CE de protección de datos, constituye el antecedente de la actual legislación, y delimita sin duda un marco regulador de protección de datos personales ineludible para el legislador español. Según ésta normativa, los Estados miembros se comprometen a garantizar *"la protección de las libertades y los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales"*. Con respecto a ello, cabe destacar que la Directiva no reduce su objeto a la tutela de la intimidad, sino que se refiere a la protección de libertades y derechos fundamentales de las personas

[64] A. HERRÁN ORTÍZ, *El derecho a la protección de datos personales en la sociedad de la información*, Universidad de Deusto, Instituto de Derechos Humanos. Cuadernos Deusto de Derechos Humanos. Núm 26. Bilbao 2003, p. 22-24

físicas, por lo tanto su protección no ampara a las personas jurídicas.[65]

Otro aspecto digno de mencionar es que la protección de las personas tiene lugar no sólo frente al tratamiento automatizado, sino frente a cualquier tratamiento automatizado o no[66]. En consecuencia la Directiva amplia el marco de garantías del derecho a la protección de datos respecto de las directrices de la OCDE y de las Naciones Unidas, así como respecto al Convenio 108, dado que sus disposiciones serán también aplicables en todo caso a los tratamientos no automatizados de datos incorporados a ficheros[67], constituyendo esto una novedad en lo que respecta al ámbito de aplicación. Según se puede apreciar en el Considerando 27 de la Directiva 95/46/CE, la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues de lo contrario daría lugar a riesgos graves de elusión; que no obstante en lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que están estructuradas.

Sin embargo, la misma Directiva establece una norma transitoria de aplicación de sus disposiciones a los ficheros manuales preexistentes, dado que los Estados miembros podrían establecer un periodo transitorio de adaptación de dichos ficheros hasta el 24 de octubre de 2007.

En el caso particular de España, la Ley 15/1999 Orgánica de Protección de Datos, ha seguido fielmente los parámetros establecidos por la Directiva en este tema, ya que prevé en sus disposición adicional primera, un plazo máximo hasta octubre del año 2007 a fin de que se lleve a cabo la adecuación de los ficheros no automatizados a la normativa, y dispone:

---

[65] A nivel europeo, se contempla cierta uniformidad legislativa en este aspecto, así, en la mayoría de los países de la Unión Europea, se encuentra reconocida sólo a personas físicas la titularidad del derecho a la protección de datos, sin embargo, cabe resaltar las legislaciones de Polonia, Italia, Dinamarca, Luxemburgo y Suiza que reconocen también a las personas jurídicas como titulares del derecho a la protección de datos de carácter personal.

[66] Este ha constituido uno de los aspectos trascendentales, que originaron la derogación de la LORTAD, ya que en la misma se regulaba únicamente a los tratamientos automatizados, estando los ficheros manuales al margen de la mencionada Ley.

[67] Esto se encuentra establecido en el artículo 3.1 de la Directiva 95/46/CE.

> *"Los ficheros y tratamientos automatizados, inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones Públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente. En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica y la obligación prevista en el párrafo anterior deberá cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados".*

Por lo tanto, de la lectura de la disposición se interpreta que los titulares de ficheros no automatizados, debían llevar a cabo la notificación para la inscripción de los mismos hasta la mencionada fecha, a fin de no incurrir en infracción.

A continuación abordaremos puntuales temas de esta nueva normativa comunitaria, la cual introduce otras importantes novedades, tal y como lo detalla Agustín Puente Escobar[68], entre ellas cabe mencionar por ejemplo, la regulación del encargado del tratamiento, el desarrollo de los principios de calidad de los datos, el interés legítimo como legitimador del tratamiento, la cláusula sobre la libertad de expresión, el reconocimiento del derecho de oposición, el reconocimiento de los derechos relacionados con las decisiones individuales automatizadas, el desarrollo de sistemas de autorregulación sectorial, el régimen sistemático de las transferencias internacionales de datos, y el reforzamiento de las funciones de las autoridades de protección de datos y creación del Grupo del artículo 29.

La Directiva diferencia claramente entre las figuras del responsable y el encargado del tratamiento, estableciendo en su artículo 17 que la elección de un encargado del tratamiento que garantice la protección de los derechos de los afectados será

[68] A. PUENTE ESCOBAR, op. cit. p.59-63

responsabilidad del responsable del fichero. Al propio tiempo, la Directiva exige que la relación existente entre el responsable y el encargado se encuentre formalizada en un contrato o acto jurídico vinculante, que deberá constar por escrito o en otra forma equivalente, imponiendo al encargado la obligación de implantar las adecuadas medidas de seguridad.

Por otro lado, en lo que se refiere a los principios de calidad de los datos, el artículo 6 de la Directiva los delimita, así como también hace referencia a los principios de tratamiento leal y lícito, finalidad y prohibición del uso incompatible, proporcionalidad, exactitud, actualización y conservación de los datos exclusivamente durante el tiempo en que sea necesario para el cumplimiento del fin.

Con respecto al interés legítimo como legitimador del tratamiento, la Directiva delimita claramente los supuestos en que podrá procederse al tratamiento de datos de carácter personal. Así, partiendo de la exigencia del consentimiento del interesado, definido por el artículo 2 h) como "*toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan*", el artículo 7 permite el tratamiento sin consentimiento del afectado pudiendo éste efectuarse solo si:

> *"a) el interesado ha dado su consentimiento de forma inequívoca, o b) es necesario para la ejecución de un contrato en que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o d) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva"*

Estos supuestos se ven reducidos en caso de tratamiento de datos sensibles (artículo 8 de la Directiva), si bien se establece una regla especial relacionada con el tratamiento de los datos de salud *"no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto*".

Por otra parte, en cuanto al deber de información a los ciudadanos acerca del tratamiento de sus datos personales, la Directiva establece la diferenciación entre los supuestos en que la información se obtiene directamente del interesado o se obtiene de terceros orígenes, en cuyo caso, será posible exceptuar este deber de información *"cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescriptos por ley"*.

Con respecto a los derechos de los ciudadanos, la Directiva, además de reconocer y regular detalladamente los derechos de acceso, rectificación y cancelación, así como el derecho de los interesados a ser indemnizados como consecuencia de los perjuicios que les fueran causados como consecuencia del tratamiento de sus datos, regula una serie de derechos de los afectados, no regulados en textos internacionales anteriormente citados.

El Artículo 9 de la Directiva, hace alusión al tratamiento de datos personales y libertad de expresión, un tema que ha sido objeto de múltiples debates, más aun, en la época actual en la que vivimos y en la cual, la libertad de prensa juega un importante papel y ejerce una importante influencia. Así pues, el mencionado precepto establece que "*en lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten*

necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión".

Se contempla en la Directiva 95/46/CE una nueva figura jurídica, el derecho de oposición, el cual se encuentra restringido a determinados supuestos, y no constituye un derecho de oposición general. Se encuentra establecido en el artículo 14 de la mencionada normativa comunitaria y presenta dos manifestaciones distintas, atendiendo al ámbito de actividad en que se produce el tratamiento. En concreto se reconoce, en primer lugar, el derecho a oponerse en los casos del artículo 7 apartados e) y f), en cualquier momento y por razones legítimas propias de su situación particular, a que sus datos sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya esos datos. El segundo lugar, la Directiva reconoce el derecho a oponerse previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos a dicha comunicación o utilización.

En el artículo 15 de la norma comunitaria objeto del presente análisis, se regulan los derechos relacionados con las denominadas decisiones personales automatizadas, las cuales, según comenta A. Herrán Ortiz[69], encuentran su más inmediato antecedente legislativo en la Ley francesa de 1978, si bien se introducen importantes novedades respecto al texto francés. Así dispone el artículo 15.1 el derecho de 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*

[69] A. HERRÁN ORTIZ, op. cit. p. 34.

de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etcétera"[70].

Este principio reconoce dos excepciones, por lo que las personas deberán someterse a decisiones individuales automatizadas cuando dicha decisión, "a) *se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguarda de su interés legítimo*; o *b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado*." A propósito de las excepciones mencionadas, se vislumbran en ellas muy poca relevancia práctica, ya que en ningún caso se traducen en garantías jurídicas importantes para el interesado. En efecto, el derecho del afectado a ser oído no establece otras consecuencias que no sean las de hacerse escuchar; por otra parte cuando el tratamiento esté autorizado, si bien se exigen garantías y medidas únicamente se indica que deberán ser "apropiadas", sin que en ningún caso se especifique en qué deberán consistir o cómo han de adoptarse tales medidas.

Es importante también destacar la relevancia del nuevo régimen que aporta esta normativa comunitaria en lo que respecta al fomento de la autorregulación. El artículo 27.1 de la Directiva dispone que *"los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de las presente Directiva*". La importancia de este precepto radica en que el mismo insta a los Estados a legislar en su ámbito interno y de esta manera lograr una homogénea aplicación de la Directiva, así también contribuye a que el derecho a la protección de datos, sea protegido y que a través de ello se fomente la creación de organismos encargados de brindar la

[70] Esta norma, según comenta la mencionada autora, provocó cierta intranquilidad a las empresas de marketing directo, ya que en consideración a estas disposiciones, se cuestionaba la licitud de las prácticas y usos de estas empresas, consistentes en seleccionar destinatarios a partir de determinada puntuación obtenida por ordenador, lo que facilita la tarea de formar listados o relaciones de destinatarios con fines de publicidad directa.

suficiente garantía a los interesados en la protección de sus datos de carácter personal en los países de la Unión Europea.

En lo que se refiere al ámbito de las transferencias internacionales, los artículos 25 y 26 de la Directiva establecen un régimen que parte del principio de que *"los Estados miembros dispondrán que la transferencia a un país tercero de datos personales, que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado*", pudiendo dicho nivel de adecuación acordarse por la Comisión, en cuyo caso, los Estados miembros no podrán denegar la transferencia con amparo en la inexistencia de un nivel adecuado de protección. Esta regla sólo podrá exceptuarse en supuestos tasados por el artículo 26 de la Directiva o, en caso de no darse los mismos, "*cuando el responsable del tratamiento ofrezca garantías suficientes respecto de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas*"[71].

La Directiva prevé la cooperación entre autoridades de los Estados miembros, creando a tal efecto un grupo específico de trabajo, regulado por su artículo 29, como órgano consultivo e independiente de los Órganos de la Unión Europea, cuyos miembros son designados directamente por las autoridades de control. Dicho Grupo tiene como funciones esenciales el intercambio de información en materia de protección de datos y deliberación de los asuntos propuestos por la Comisión o los propios miembros. El papel de este Grupo, ha resultado esencial en el desarrollo e interpretación de las normas de protección de datos, tanto en el análisis del nivel de protección de datos personales en terceros Estados como en cuanto al estudio sistemático de la

[71] En los últimos años ha sido fundamental el papel de la Comisión y del Grupo del artículo 29 de la Directiva en la preparación y aprobación de modelos de cláusulas contractuales tipo, para las transferencias internacionales de datos a terceros Estados que no ofrecen un nivel adecuado de protección.

aplicación de las normas de protección de datos a tratamientos concretos.

Como manifiesta Puente Escobar[72], la importancia de este instrumento comunitario es fundamental en la regulación actual de protección de datos de carácter personal, no solo en el ámbito europeo, sino también en el mundial, dado que las normas de la misma en materia de transferencias internacionales de datos vienen a imponer un régimen básico al que deberán resultar "adecuados" los terceros Estados no miembros de la Unión, para que los datos puedan ser transmitidos libremente a esos Estados.

VI. La Ley 15/1999, de1 3 de diciembre, de Protección de Datos de Carácter Personal:

El texto que fue presentado por el Gobierno para la adaptación de la LORTAD a la Directiva constituía en un principio una reforma de la misma sin que se contemplara la redacción de una nueva norma. No obstante, el elevado número de enmiendas a dicho texto, en total ciento catorce, provocó que se propusiera un nuevo texto legal con el objeto de derogar el anterior.

La LOPD que entró en vigencia el 14 de enero del año 2000, consta de siete títulos, cuarenta y nueve artículos, seis disposiciones adicionales, tres disposiciones transitorias, una derogatoria y tres disposiciones finales. La falta de una exposición de motivos, resulta sorprendente; siguiendo las ideas de Greixas Gutiérrez[73] es posible afirmar que si bien el anteproyecto si contaba con una, que se encontraba prevista inicialmente, ésta hacía referencia únicamente a la adaptación a la Directiva 95/46/CE, de 24 de octubre, sin embargo, ella fue desapareciendo a medida que la ley fue superando los diversos trámites parlamentarios. Esta omisión puede ser criticada como un punto negativo de la nueva Ley, ya que la existencia de una exposición de motivos permitiría profundizar sobre las innovaciones introducidas y aclarar el contenido de la disposición en todas aquellas cuestiones dudosas

[72] A. PUENTE ESCOBAR, op. cit. p.59

[73] G. FREIXAS GUTIÉRREZ, *La protección de los datos de carácter personal en el derecho español*, Bosch, Barcelona, 2001, p.83-84

que podrían ser interpretadas al amparo de ella, todo lo cual se pierde con la ausencia de ésta.

Por otro lado, observando los aspectos positivos de ésta norma, es digno de destacar que en la LOPD aparecen nuevos aspectos que no habían sido contemplados en la LORTAD. En primer lugar, la ampliación del objeto de la Ley, ya que se incluyen los ficheros manuales estructurados. Con la transposición de la Directiva, ya no sólo se persigue la protección de la intimidad y de los derechos y libertades de los titulares de los datos sino también el respeto a las libertades y derechos fundamentales de las personas físicas y en especial de su intimidad. Esto significa que se intenta evitar que a través del conocimiento de aspectos personales de un individuo se vulneren sus derechos fundamentales.

En cuanto al ámbito geográfico de aplicación de la norma éste no sólo afecta a los tratamientos que tengan lugar en territorio español y cuyo responsable esté establecido en el mismo, también cuando aún no estando establecido en territorio español, en aplicación de las normas de Derecho Internacional Público le sea aplicable la legislación española. Asimismo, cuando el responsable no esté situado en territorio español o de la Unión Europea pero utilice para el tratamiento medios situados en el territorio español, a excepción de que sean utilizados con fines de tránsito. Con la nueva norma se reduce el número de ficheros que quedan fuera del ámbito de la normativa relativa a protección de datos pasando de cinco a tres.

Con respecto a las definiciones previstas en la LOPD, luego de realizar un análisis comparativo con la LORTAD, se aprecia un aumento de las mismas, siendo destacable la inclusión del término consentimiento, del concepto de fuentes accesibles al público enumerando taxativamente qué tipo de ficheros deben considerarse como tal, de igual modo se introdujo un nuevo sujeto pasivo del régimen sancionador, el encargado del tratamiento.

1. Objeto de protección de la LOPD:

El artículo primero de la Ley 15/1999, de Protección de Datos Personales establece que su objeto es garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades

públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal.

Según Garriga Domínguez[74], sin duda alguna, este artículo se encuentra en su redacción, evidentemente influido por la Directiva 95/46/CE, la cual dispone que su primer objetivo será la protección de los derechos y libertades de las personas físicas, siguiendo la tradición marcada por el Convenio de 28 de enero de 1981 del Consejo de Europa y también por otras normas de protección de datos personales anteriores, cuya aprobación responde a la necesidad de proteger los derechos fundamentales de las personas en lo que respecta al tratamiento de sus datos personales.

Del análisis del artículo primero de la Ley puede deducirse que lo relevante ahora, más que limitar la informática, es garantizar de forma efectiva los derechos fundamentales de la persona. Sin embargo, resulta pertinente no olvidar que el objeto de limitar la informática en la LORTAD era también garantizar esos mismos derechos. Por lo tanto, y pese a reconocer que la nueva redacción mejora la anterior por cuanto parece que ahora sí, lo importante es la libertad y dignidad de la persona, en nada se habrá avanzado si los derechos de los afectados no gozan de plena eficacia frente a la anterior regulación caracterizada por las numerosas excepciones a aquellos.

Siguiendo la postura de la autora más arriba citada, es posible concluir que el objeto de la LOPD no es otro que el desarrollo del contenido y elementos del derecho a la autodeterminación informativa, así como el establecimiento de las garantías necesarias para su protección. A través de la limitación del tratamiento de los datos de carácter personal, primer objeto de protección en la Ley, se intenta conseguir la salvaguardia de esa esfera de la libertad de las personas que se denomina autodeterminación informativa o libertad informática. Por lo tanto la finalidad de la Ley no es proteger los datos personales de los ciudadanos, sino la protección de éstos en relación con el tratamiento de los mismos, para salvaguardar el último término la libertad de la persona y posibilitar su desarrollo sin interferencias.

[74] A. GARRIGA DOMÍNGUEZ, *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid 2004. p.51

2. Titulares del derecho a la autodeterminación informativa en la LOPD:

Ha surgido un interesante debate entorno al reconocimiento de la existencia o no del derecho a la autodeterminación informativa a las personas jurídicas. Son numerosos los autores que argumentan que solo las personas físicas pueden ser titulares de este derecho, excluyendo así a las personas de existencia ideal, y así lo establece también la Ley Orgánica, al disponer que su objeto es el de garantizar los derechos y libertades de las personas físicas.[75]

La Agencia Española de Protección de Datos se ha pronunciado también al respecto, así encontramos la Resolución de 27 de febrero de 2001, recaída en el expediente iniciado como consecuencia de la denuncia efectuada a una determinada Cámara de Comercio como consecuencia de la transmisión a terceros de los datos contenidos en el censo público regulado por la Ley 3/1993. La citada Resolución acuerda el archivo del expediente, indicando en su Fundamento Jurídico II que: "*... la protección conferida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, no es aplicable a las personas jurídicas, que no gozarán de ninguna de las garantías establecidas en la Ley, y por extensión lo mismo ocurrirá con los profesionales que organizan su actividad bajo la forma de empresa (ostentando, en consecuencia la condición de comerciante a la que se refieren los artículos primero y siguientes del Código de Comercio) y con los empresarios individuales que ejercen una actividad comercial y respecto de las cuales sea posible diferenciar su actividad mercantil de su propia actividad privada, estando en el primer caso excluidos también del ámbito de aplicación de la Ley Orgánica 15/1999. En definitiva pues, tanto las personas jurídicas como los profesionales y los comerciantes individuales (estos dos últimos sólo en los estrictos términos señalados en el párrafo que antecede, esto es, cuando sus datos hayan sido tratados tan sólo en su consideración de empresarios) quedan fuera del manto protector de la Ley Orgánica 15/1999..*".

En el marco de la doctrina española se manejan a su vez, otros argumentos para oponerse a la extensión de las personas jurídicas como sujetos activos titulares en materia de protección de datos.

[75] Artículo 1 de la Ley 15/1999 Orgánica de Protección de Datos.

Siguiendo esta teoría, afirma Davara Rodríguez[76], que el afectado o interesado es la persona física, titular de los datos que sean objeto de tratamiento; con respecto a ello, la protección de las personas jurídicas se encuentra más cómodamente encuadrada en el derecho de sociedades, en las legislaciones sobre patentes y marcas, en defensa de la competencia, en los derechos de autor y en otras varias. Éste autor, considera que incluir en la misma protección, bajo los conceptos de datos personales e intimidad, a las personas físicas y a las jurídicas resulta muy poco práctico.

Por otro lado, se ha afirmado que los bienes, derechos o intereses que se tutelan en el caso de las personas físicas y en el de las jurídicas son diferentes, por lo tanto la protección que se debe otorgar a las personas físicas y a las personas jurídicas ha de ser diferente. Así, mientras en las personas físicas lo que se protege es su privacidad, en las personas jurídicas lo que se protege es su publicidad.

Por otro lado, hay una floreciente doctrina que alienta el reconocimiento del derecho a la protección de datos personales de las personas jurídicas. Entre los autores que siguen esta teoría encontramos a Lucas Murillo de la Cueva[77], quien sostiene que el reconocimiento de las personas jurídicas como sujetos activos del derecho a la autodeterminación informativa permitirá realizar una mejor defensa de sus miembros cuando los datos que se refieran a la composición y/o actividad de aquellas sean objeto de tratamiento informático. Según este autor, erigir a un ente moral como titular del derecho a la autodeterminación informativa supone elevar un primer mecanismo de protección de sus socios, más fácil de activar, pues lo pueden ejercer los órganos sociales y de eficacia más amplia, ya que el ejercicio del derecho por la persona jurídica beneficia a todos sus componentes a la vez.

Siguiendo ésta tesitura, Garriga Domínguez[78], expone otro argumento a favor de extender la titularidad del derecho a la autodeterminación informativa a las personas jurídicas, éste se basa en el peligro real de que conductas prohibidas por la Ley de

[76] M. A. DAVARA RODRÍGUEZ, La protección de datos en Europa. Principios, derechos y procedimiento, ASNEF-EQUIFAX Madrid, 1998. p. 94-95
[77] P. LUCAS MURILLO DE LA CUEVA, op. cit. p.182
[78] A. GARRIGA DOMÍNGUEZ, op. cit. p.69-72.

Protección de Datos afecte a los relativos a una persona jurídica y, no gozando ésta de los derechos garantizados en ella, ni estando amparada por los principios que los inspiran, difícilmente podrán defenderse.[79]

Se debe reconocer que el derecho a la protección de datos busca proteger la vida privada y la intimidad, derechos que son difíciles de extender a las personas jurídicas, ya que siempre han sido concebidas en función de las personas individuales. Sin embargo, si se considera a las personas de existencia ideal como titulares de un derecho autónomo y diferente al de la intimidad como lo es el derecho a la autodeterminación informativa, se facilita la inclusión de aquellas dentro del objeto de aplicación de las leyes de protección de datos.

El Tribunal Constitucional se ha pronunciado en varias oportunidades con respecto a los derechos que asisten a las personas jurídicas. En la Sentencia 53/1983, de 20 de junio, les ha reconocido legitimación para accionar con base en el artículo 24.1, el derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos.

Más específicamente, en lo que se refiere al tema tratado en este apartado, encontramos la Sentencia 120/1983, de 15 de diciembre, a través de la cual se les reconoce a las personas jurídicas la posibilidad de ser titulares del derecho al honor. Sin embargo, no siempre la postura del Tribunal Constitucional ha sido uniforme a este respecto, ya que en otras ocasiones, como lo comenta Garriga Domínguez[80], se ha mostrado rotundo a la hora de negar a las personas jurídicas la titularidad de determinados derechos fundamentales. Tal es el caso del derecho a la intimidad o del derecho a la propia imagen.

---

[79] Esta problemática ha llegado también al Tribunal Constitucional, habiéndola abordado en varias ocasiones. Sin embargo, no en todas ellas ha habido una misma respuesta, sino que ésta va a depender del derecho fundamental de que se trate en cada caso concreto. Cabe mencionar la Sentencia 19/1983, de 14 de marzo, habiéndosele planteado al Tribunal Constitucional la posibilidad de que las personas jurídicas pudieran ser titulares del derecho contenido en el artículo 53.2 de la Constitución, entiende que "*basta leer los artículos 14 a 29 para deducir el sentido del artículo 53.2, que es el afirmar que cualquier ciudadanazo puede recabar la tutela de tales libertades y derechos, es decir, que todos los ciudadanos son titulares de los mismos, pero sin que ello limite la posible titularidad de otras personas*"

[80] A. GARRIGA DOMÍNGUEZ, op. cit. p. 71

Cabría analizar con detalle si la tutela que merecen las personas jurídicas puede ser la de un derecho humano, es decir, ¿Cabría modificar la Ley Orgánica 15/1999, la cual regula el derecho fundamental previsto en el artículo 18.4 de la Constitución Española, a fin de incluir a las personas jurídicas como titulares del derecho a la autodeterminación informativa?[81] Si se procediera a ello, la Ley 15/1999 no sería la primera Ley Orgánica que reconociera a las personas como titulares de un derecho fundamental, tal es el caso de la Ley Orgánica 2/1984 de 26 de marzo, reguladora del derecho de rectificación. La misma establece en su artículo primero que *"toda persona natural o jurídica, tiene derecho a rectificar la información difundida, por cualquier medio de comunicación social, de hechos que le aludan, que considera inexactos y cuya divulgación pueda causarle perjuicio."*

Es menester considerar que tanto las personas físicas como jurídicas pueden tener interés en ejercitar el derecho de acceso, de rectificación o de cancelación de datos inexactos, falsos o desfasados, y si las personas de existencia ideal tienen la potestad de ejercer su derecho de rectificación ante los medio de comunicación, también deberían tener la facultad para reclamar el acceso, rectificación o cancelación de sus datos de carácter personal.

Siguiendo esta misma postura, que ve justificado el reconocimiento del derecho a la autodeterminación informativa a las personas jurídicas, Hernando Collazos[82] manifiesta que tanto éstas como las personas físicas tienen interés en obtener rectificación de sus datos equivocados que figuran en ficheros públicos y privados. Como ejemplo, la autora cita las reivindicaciones expresadas por las pequeñas y medianas empresas que desean poder ejercer un derecho de acceso a los ficheros bancarios, en casos de denegación de un crédito o de facilidades

[81]La Constitución Española recoge algunos temas que deben regularse por este procedimiento, como son las Leyes de desarrollo de los Derechos Fundamentales y de las Libertades Públicas recogidas en la sección primera del capítulo segundo del Título I de la Constitución, las que aprueban los Estatutos de Autonomía y las demás previstas en la Constitución.

[82] I. HERNANDO COLLAZOS, *La Comunidad Económica Europea y la informática.* Jornadas Internacionales sobre Informática y Administración Pública, Instituto Vasco de Administración Pública. Volumen 3. VVAA. Bilbao 1986 p.90

diversas, sin que conozcan los motivos verdaderos y no dispongan de los medios jurídicos para contestarlos.

Con respecto a las personas fallecidas, han surgido también varias dudas en lo que se refiere a la aplicación de la Ley Orgánica, es por ello que cabría plantearnos la siguiente interrogante, ¿tienen las personas fallecidas derecho a la autodeterminación informativa? la solución deberá estar en función de la naturaleza misma del derecho protegido por la norma, lo que conlleva a la necesidad de determinar si la muerte de las personas da lugar a la extinción del derecho a la protección de sus datos personales, ya que el artículo 32 del Código Civil dispone que " la personalidad civil se extingue por la muerte de las personas", lo que determinaría, en principio, la extinción con la muerte de los derechos inherentes a la personalidad.

Sin embargo cabe analizar profundamente este tema, ya que sin perjuicio de lo anteriormente expuesto, debe indicarse que la protección otorgada por la Ley frente a las intromisiones que supongan una vulneración de los derechos al honor y a la intimidad subsiste con posterioridad a la muerte de las personas. En ese sentido, cabe destacar que la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pone de manifiesto en sus artículos 4 a 6 que el fallecimiento no impide que por las personas que enumera el primero de los preceptos citados puedan ejercitarse las acciones correspondientes, siendo éstas la persona que el difunto haya designado a tal efecto en testamento, su cónyuge, ascendientes, descendientes o hermanos que viviesen al tiempo de su fallecimiento o, a falta de las personas anteriormente citadas, el Ministerio Fiscal.

Teniendo en cuenta lo anteriormente expuesto, la LOPD tiene como objeto especial (por imperativo del artículo 18.4 de la Constitución) la protección del honor y la intimidad, estableciendo a lo largo de su articulado las medidas precisas para asegurar que dicha protección se lleva plenamente a efecto.

Luego del análisis conjunto de las disposiciones contenidas en ambas Leyes se desprende que la legitimación conferida para el ejercicio de las acciones reconocidas en la Ley Orgánica 1/1982

existirá, en el ámbito de la LOPD, cuando la actuación de las personas legitimadas tenga por directo y exclusivo objeto el ejercicio de las acciones tendentes a la protección del honor, la intimidad personal y familiar y la propia imagen de las personas fallecidas, no siendo posible la actuación de éstas en cualquier otro supuesto en que la finalidad de su actividad difiera de la antedicha protección. Por lo tanto, en el caso de que los familiares de una persona fallecida quisieran ejercer en nombre de ésta última su derecho a la autodeterminación informativa, la ley no los legitimará para ello, cuando se refiera a datos que no necesariamente afecten el honor o la intimidad del fallecido.

Ello supone que, en principio las personas legitimadas por la Ley Orgánica 1/1982 carecerán de legitimación para el ejercicio de los derechos reconocidos por la LOPD, salvo en los supuestos en que esos derechos se ejerciten como instrumento para la realización de alguna de las finalidades protectoras indicadas que la Ley Orgánica 1/1982 les atribuye. Fuera de estos supuestos no será posible entender que la actividad de los herederos o personas referidas en el artículo 4 de la Ley Orgánica 1/1982 se encuentra amparada por la LOPD. En consecuencia, los datos de las personas fallecidas no entran dentro del amparo de la LOPD ni de los reglamentos que la desarrollan.

Esta es también la línea de interpretación que sigue la Agencia Española de Protección de Datos[83], con respecto a los derechos de las personas fallecidas, la misma considera que el ejercicio del derecho a la protección de datos personales, es “personalísimo”, y sólo la persona afectada puede ejercerlo, no así sus familiares.

[83] En lo que respecta al derecho comparado en esta materia a nivel europeo, se puede afirmar que existe uniformidad en la interpretación de este tema. Siendo destacable el caso de Islandia que prevé como objeto de protección los datos de personas tanto vivas como fallecidas.

CAPÍTULO III
PRINCIPIOS RECTORES DEL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL Y DERECHOS DEL INTERESADO

I. Principios rectores del tratamiento automatizado de datos de carácter personal:

Los principios esenciales del derecho a la autodeterminación informativa, tales como los de proporcionalidad, tratamiento leal y lícito, finalidad, conservación o exactitud se vieron incorporados por primera vez en 1973 y 1974 en las Resoluciones 22/73 y 29/74, del Consejo de Europa[84], referidas respectivamente a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos de los sectores privado y público.

Con respecto a España, la exposición de motivos de la derogada LORTAD definía los principios de la siguiente manera:

> *"Los principios generales, por su parte definen las pautas a las que debe atenerse la recogida de datos de carácter personal, pautas encaminadas a garantizar tanto la veracidad de la información contenida en los datos almacenados cuanto la congruencia y racionalidad de la utilización de los datos".*

Si bien la normativa vigente[85] no cuenta con exposición de motivos que aclare la función que cumplen los principios como bien lo hacía la anterior Ley 5/1992, la LOPD regula en su título segundo, artículo cuarto, ***la calidad de los datos***, para lo cual establece los principios generales de la protección de datos, que inspiran la regulación de los ficheros en los cuales se encuentran almacenados los datos personales, que deben regir todas las operaciones de tratamiento y cesión de datos de carácter personal, que se desarrollan a continuación.

[84] Cabe resaltar que el Consejo de Europa ha tenido una importante participación en lo que se refiere al estudio de esta materia.
[85] La Ley 15/1999 Orgánica de Protección de Datos de Carácter Personal

1. Principios de pertinencia y finalidad:

El principio de pertinencia exige que los datos personales estén relacionados con el fin perseguido por lo que deberán, como afirma Pérez Luño, ser *"adecuados y no excederán de las finalidades para las que se hayan registrado"*[86]. Esto significa que no podrán ***solicitarse*** ni registrarse más datos que los estrictamente necesarios para llevar a cabo la finalidad de que se trate, aunque fuesen susceptibles de serlo para cumplir objetivos futuros.

Por lo tanto, la persona a la cual se le requieran datos que resulten excesivos, podrá negarse a suministrarlos, amparándose en el artículo 4.1 de la LOPD que establece que: *"Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando* ***sean adecuados, pertinentes y no excesivos en relación con el ámbito*** *y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido"*.

Una vez que se obtengan los datos, según el principio de finalidad, no podrán ***ser utilizados*** con fines diferentes a los que motivaron la recogida, ya que el artículo 4.2 de la Ley establece que "*los datos de carácter personal objeto de tratamiento, no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos."* Por lo tanto, una vez que hayan sido recabados los datos necesarios, estos no podrán ser utilizados para cumplir objetivos diferentes al inicial, salvo que por intereses superiores, pudiendo reconocerse la excepción de ser utilizados con fines en provecho de la sociedad, como ser los históricos, estadísticos y científicos, siguiendo de esta forma lo que establece la Directiva 95/46/CE, que también establece esa excepción a la regla[87].

---

[86] A. E. PÉREZ LUÑO, *Derechos Humanos en la Sociedad Tecnológica*, en M. LOSANO, y otros: Libertad informática y leyes de protección de datos, Centro de Estudios Constitucionales, Madrid 1990 p. 166

[87] Esto se encuentra contemplado en el artículo 6.1 b), que dispone lo siguiente: *"Los Estados miembros dispondrán que los datos personales sean recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas"*. Aquí cabe hacer hincapié, en que si bien la Directiva reconoce la excepción en los casos mencionados, estipula también que para que ello sea posible, el Estado deberá ofrecer

Cabe agregar que, en lo que respecta a la cesión, los datos podrán ser comunicados a un tercero únicamente para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado, según lo establece el artículo 11.1 de la LOPD.

Del análisis del principio de finalidad, es posible inferir que éste se encuentra íntimamente conectado con el principio de pertinencia, hasta el punto de que el cumplimiento del segundo implica necesariamente el respeto al primero, ya que los datos han de ser adecuados para una finalidad concreta.

Garriga Domínguez[88], realiza una comparación entre el principio de pertinencia y el de finalidad, manifestando que éste último, difiere del primero en cuanto a su amplitud de contenido, ya que aporta el requisito de que los datos deberán ser usados exclusivamente para la finalidad para la que fueron recabados, y aclarando que ésta deberá ser respetuosa con el ordenamiento jurídico, por lo tanto esta finalidad deberá ser legítima, explícita y determinada, debiendo definirse de la forma más precisa posible y el uso que se haga de esos datos con posterioridad, deberá ser compatible con la finalidad de la recogida de los mismos.

El artículo 4.5 de la LOPD establece en este sentido que *"los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados"*. Esto significa que una vez cumplida la finalidad para la cual los datos fueron recogidos, deberán éstos ser cancelados[89], lo cual permite que los datos no sean conservados por más tiempo de lo necesario, una vez que se haya cumplido la finalidad para la cual fueron recabados.

2. Principios de veracidad y exactitud:

Estos principios se desprenden del artículo 4.3 de la LOPD, que dispone: *"los datos de carácter personal serán exactos y puestos*

las garantías suficientes a los ciudadanos a fin de que se encuentren protegidos en sus derechos.

[88] A. GARRIGA DOMÍNGUEZ, *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid 2004. p.79

[89] Según lo prescribe el Artículo 4.4 de la Ley 15/1999 Orgánica de Protección de Datos.

al día de forma que respondan con veracidad a la situación actual del afectado". De ello se infiere que una vez que los datos se encuentren recabados, el responsable del fichero estará obligado a mantenerlos al día, es decir, asegurarse de que sean exactos y verdaderos, debiéndose realizar las actualizaciones correspondientes cuando sean pertinentes.

Por lo tanto, los datos deberán ser exactos a fin de que correspondan fielmente a la situación del afectado, ya que como expone Herrán Ortiz, si éstos resultaran inexactos, en todo o en parte, o incompletos, no se justificaría su tratamiento ya que esto se produce sólo cuando la información tratada responde con la veracidad y exactitud de la situación actual de la persona. Esto obligaría a que deban ser cancelados y sustituidos de oficio los datos inexactos por aquellos que se encuentren rectificados o completados, sin perjuicio de la facultades que tengan reconocidas los afectados.

Si es importante reconocer la relevancia de este principio, es también verdad que esta garantía no es suficiente para asegurar el cumplimiento de la obligación que contempla el mismo, ya que según como comenta Freixas Gutiérrez[90], podría darse el caso de que los responsables de los ficheros desconozcan la evolución de algunos datos; por lo que la Ley prevé el complemento de este principio con los derechos de acceso, rectificación y cancelación previstos en el artículo 16 de la LOPD.

A éste respecto se ha pronunciado el Tribunal Constitucional, que en su Sentencia 105/1990[91], de 6 de junio, ha manifestado que el requisito constitucional de veracidad supone que *"el informador tiene (…) un especial deber de comprobar la veracidad de los hechos que expone mediante las oportunas averiguaciones, y empleando la diligencia exigible a un profesional"*. Si bien esta Resolución ha resuelto un recurso amparo que se planteaba en el marco de la defensa del derecho al honor, puede ser también aplicada en el marco de la defensa del derecho a la autodeterminación

[90] G. FREIXAS GUTIÉRREZ, *La protección de datos de carácter personal en el derecho español*, Bosh, Barcelona. 2001 p.160

[91] En su Fundamento Jurídico Número 5.

informativa en el caso de que no se cumpla con el principio de veracidad establecido por el artículo 4.3, más arriba mencionado.

3. Principio de lealtad:

Este principio se inspira en el artículo 4.7 de la LOPD, el cual establece que *"Se prohíbe la recogida de datos por medios fraudulentos, **desleales** o ilícitos"*. En base a este principio, se infiere que los datos personales deberán recogerse sin engaños o falsedades por parte de quien los solicita, prohibiendo la Ley de forma contundente la utilización de medios fraudulentos, desleales o ilícitos.

En lo que respecta a la recogida fraudulenta de datos de carácter personal, la Agencia Española de Protección de Datos ha dictado numerosas Resoluciones Sancionadoras por incumplimiento del artículo 4.7. Entre ellas se destaca la Resolución: R/00021/2007[92] en la cual se señala que "*la obligación establecida en el citado artículo 4.7 impone la necesidad de que los datos personales que se recojan en cualquier fichero sean obtenidos por medios lícitos, y de esta forma, sea conocida su utilización por los afectados, siendo los responsables de su obtención quienes responden del cumplimiento de esta obligación*".

Por otro lado, la Audiencia Nacional en su Sentencia de 9/03/06[93], en cuanto a la aplicación del citado precepto ha señalado que *"…la inserción de los datos personales en un contrato… acompañándolo de una firma falsa, sin la voluntad del afectado, supone un acto de recogida de datos fraudulenta…"*. En este sentido, la citada Sentencia menciona que *"la infracción administrativa se comete no sólo realizando los actos instrumentales de recogida fraudulenta de datos (…) sino también no impidiendo que se haga este tipo de recogida a través de procedimientos de control, cuando hay obligación de hacerlo"*.

[92] En el procedimiento sancionador PS/00097/2006, instruido a la entidad GAS NATURAL SERVICIOS, S.D.G., S.A., y a GRUPO A FIELD MARKETING IBERIA S.L., vista la denuncia presentada por D. A.F.P., D. P.S.G., D. M.N.G., DÑA. A.G.M., D. J.A.N., D. G.B.R., D. A.G.M., D. D.F.A., y D. A.B.G.,

[93] De la Sala de lo Contencioso- Administrativo, sección primera. Sobre Recogida fraudulenta de datos personales, que resuelve el Recurso contencioso-administrativo núm. 610/04.

A todo esto cabe agregar que el artículo mencionado más arriba, se encuentra en concordancia con el artículo 44.4.a), el cual considera la recogida de datos de forma engañosa y fraudulenta, como una infracción muy grave. Cabe advertir que el principio de lealtad previsto en el artículo 4.7 se encuentra relacionado también con el derecho de información previsto en el artículo 5 de la Ley 15/1999, que asiste a los interesados a la hora de recabar sus datos, previniendo la recogida de datos para fines contrarios a la voluntad del interesado.

4. Principio de seguridad de los datos:

Este principio se desprende de la obligación que tiene el responsable del fichero de proveer las medidas de seguridad necesarias a los datos de carácter personal. Esto se encuentra contemplado en el artículo 9 de la LOPD, el cual dispone que: *1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.*

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Las medidas de seguridad se encuentran también reguladas por el Real Decreto 994/99, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados[94] que contengan datos de carácter personal, en el

[94] Es pertinente realizar una aclaración en lo que respecta a la aplicación del Reglamento de Seguridad a los ficheros en soporte no automatizado. El artículo 1 del Reglamento delimita su ámbito de aplicación estableciendo que será aplicable únicamente a los ficheros

cual se establece la obligación, por parte de los titulares de ficheros públicos y privados, de velar por la seguridad de dichos ficheros y de los datos en ellos contenidos, resultando aplicable dicha exigencia a todo tipo de datos de carácter personal registrado en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado, con las excepciones que la propia LOPD establece.

El Real Decreto, mencionado *up supra,* tiene por objetivo establecer medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica de Protección de Datos. Dicho Reglamento define de forma exhaustiva lo que debe entenderse por "Sistema de información", "Usuario", "Recurso", "Accesos autorizados", "Identificación", "Autenticación", "Control de acceso", "Contraseña", "Incidencia", "Soporte", "Responsable de seguridad" y "Copia de respaldo".

También encontramos en ese texto legal, la clasificación de medidas de seguridad en tres niveles distintos; tales como el básico, el medio y el alto. Estos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

---

automatizados. Esta delimitación resultaba congruente con el sistema de garantías contemplado en la Ley Orgánica 5/1992, de 29 de octubre (LORTAD), en cuyo desarrollo fue aprobado, y que sólo era de aplicación a ficheros automatizados. La Disposición Transitoria Tercera de la LOPD mantiene la vigencia de las normas reglamentarias preexistentes, entre las que se cita el Reglamento de Medidas de Seguridad, en cuanto no se oponga a la nueva Ley. La previsión del Reglamento de aplicarse sólo a los ficheros automatizados se opone a la vigente LOPD, al haberse ampliado su ámbito de aplicación, como se ha expuesto, por lo que debe considerarse derogada En consecuencia, desde la entrada en vigor de la LOPD, resulta aplicable dicho Reglamento a los ficheros en soporte no automatizado que se hubieran creado con posterioridad a la entrada en vigor de la Ley Orgánica, el 14 de enero de 2000. Los ficheros en soportes no automatizados que existieran antes de dicha fecha dispondrán, a estos efectos, del período de adaptación establecido en la Disposición Adicional Primera (que finaliza en octubre de 2007).

Según lo expone Cueva Calabia[95], ha crecido en los últimos años la importancia del principio de seguridad, en orden a garantizar los derechos de los afectados, al mismo tiempo que se ha producido microelectrónica y el software, lo que ha permitido la proliferación de sistemas informáticos potentes y fáciles de utilizar, se han incrementado "*los riesgos que amenazan a los datos almacenados y procesados por ellos y, en consecuencia, a los ciudadanos a quienes dichos datos conciernen*". Es por ello que las medidas de seguridad deben actualizarse a las exigencias que surgen en el presente, a fin de lograr la protección adecuada que requieren los datos de carácter personal.

Es menester hacer hincapié en la postura defendida por Garriga Domínguez[96], quien sostiene que el principio de seguridad y los demás principios de calidad de los datos, responden a la finalidad general de encontrar un equilibrio adecuado entre el respeto a los derechos de las personas y la utilización y circulación de la información personal. El individuo, en la medida en que se desenvuelve dentro de la comunidad social, no posee un derecho absoluto e ilimitado sobre sus datos, pero sí es titular del derecho a que la "utilidad social" de sus datos personales respete unos límites que garanticen sus derechos fundamentales.

II. Derechos del Interesado:

Una vez realizada la exposición de los principios rectores del derecho a la autodeterminación informativa, es necesario desarrollar los derechos que permiten que ellos no queden reducidos a meras normas y criterios programáticos. Justamente por su especial trascendencia en la garantía y tutela de la autodeterminación informativa, se hace precisa una delimitación y análisis práctico del contenido del ejercicio y alcance de los derechos que reconocidos al interesado en la LOPD, le permiten una defensa legal de su derecho a la protección de datos personales.

[95] J. L CUEVA CALABIA, *La LORTAD y la seguridad de los sistemas automatizados de datos personales, en la Actualidad Informática* Aranzadi, número 13, octubre, Aranzadi, 1994, p.7
[96] A. GARRIGA DOMÍNGUEZ, op. cit. p.84

Estos derechos que forman parte del contenido esencial de la protección de datos son independientes, y el ejercicio de ninguno de ellos es requisito previo para el ejercicio de otro derecho, según la Norma Segunda de la Instrucción 1/1998 de la Agencia Española de Protección de Datos, sobre el ejercicio de los derechos de acceso, rectificación y cancelación. Los derechos que reconoce al ciudadano la Ley 15/1999 se encuentran recogidos en sus Títulos II y III, los cuales se analizan con detalle a continuación.

1. Derecho de impugnación de valoraciones basadas en tratamiento de datos:

Así como también lo disponía la derogada Ley Orgánica 5/1992 (LORTAD), la LOPD también introduce la posibilidad de impugnar valoraciones de comportamientos basadas en un tratamiento de datos personales, aunque se puede notar algunas diferencias importantes en la redacción de ambos artículos. Vemos regulado este derecho en el artículo 13.1 de la LOPD que establece que *"los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad"*.

De la lectura del apartado primero del artículo 13 se desprende que está condicionado a dos supuestos; uno de los cuales es que las decisiones adoptadas tengan efectos jurídicos, como bien lo señala Freixas Gutiérrez[97], la terminología ***efectos jurídicos*** produce cierta confusión ya que su interpretación puede hacerse desde un punto de vista restrictivo, que produzca derechos y obligaciones a los ciudadanos, o desde un punto de vista amplio, que afecte desde cualquier punto de vista la esfera personal de los derechos fundamentales de las personas y las libertades públicas. De acuerdo con el artículo primero de la LOPD[98], cabe realizar una interpretación amplia y cualquier decisión que incida en el ámbito de actuación de los ciudadanos tendrá efectos jurídicos. El segundo supuesto se refiere a que la decisión adoptada ***les afecte de manera***

[97] G. FREIXAS GUTIÉRREZ, op. cit. p. 182

[98] *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar"*.

significativa; nuevamente nos encontramos ante un concepto jurídico indeterminado y de una enorme subjetividad dado que la afectación prevista puede analizarse desde muchos puntos de vista.

En el segundo apartado del artículo 13 de la LOPD la facultad de *"impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad"*. Es posible notar la rigidez de los términos que emplea en este caso la norma, lo cual puede significar en la práctica un obstáculo insuperable para el reconocimiento de la facultad de impugnar dichos actos; en efecto, obsérvese que el legislador exige que el acto susceptible de impugnación tenga como *"único fundamento"* un tratamiento de datos que ofrezca una delimitación de la personalidad, circunstancia que hace difícil el ejercicio de este derecho, por cuanto que no será sencillo acreditar que dicho tratamiento de datos ha sido el único elemento considerado.

Hallándose la persona ante las circunstancias más arriba mencionadas, ésta podrá ejercitar su derecho establecido en el artículo 13.3 de la LOPD, el cual dispone que *"el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consista el acto*".

Finalmente, se introduce en el apartado cuarto del artículo 13 de la LOPD una garantía para los afectados según la cual "la valoración sobre el comportamiento de los ciudadanos, basada exclusivamente en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del interesado". Esto supone una novedad respecto de la derogada LORTAD, sin embargo será únicamente el afectado quien podrá solicitar este valor probatorio con lo que cualquier negativa impedirá dicha utilización.

Han sido numerosas las críticas que ha merecido la regulación de la LOPD en el ámbito de la decisiones individuales automatizadas centradas principalmente, en su falta de coherencia con lo dispuesto en el texto comunitario; entre ellas la que expone

Herrán Ortiz[99], que objeta al texto español que no se haya mostrado más explícito en el reconocimiento de un derecho de impugnación de estas decisiones, al tiempo que debiera haber establecido un derecho de información obligatorio sobre los criterios y juicios de valoración, como complemento insalvable e ineludible para que el interesado pudiera impugnar con garantías los actos que le perjudican.

El precepto presenta, a su vez, cierta falta de coherencia con respecto a la Directiva 95/46/CE en su artículo 15.2[100], ya que no se han trasladado al texto español las excepciones que éste introduce, y por las que se permite que una persona puede verse afectada por las denominadas decisiones individuales automatizadas si dicha circunstancia se halla autorizada en la ley, o si se han adoptado en el marco de la celebración de un contrato.

2. El derecho a una protección especial de los datos sensibles:

Las informaciones sensibles son aquellas que se refieren a cuestiones íntimamente ligadas al núcleo de la personalidad y de la dignidad humana. Por ello, las posibles agresiones a la libertad, a la intimidad, las posibilidades de ser discriminado o cualquier otra contra el ejercicio de los derechos fundamentales de las personas, se verían agravadas cuando los datos tratados pertenecen a la categoría de los denominados "s*ensibles*"[101].

El artículo 7 de la LOPD, sobre datos especialmente protegidos, regula la correcta protección que estos, del mismo es posible distinguir tres grupos o categorías de datos que, por

[99] A. I. HERRÁN ORTÍZ, *Los derechos de las personas en la Ley Orgánica 15/1999, de 13 de diciembre de diciembre, de Protección de Datos de Carácter Personal*. En los XVII Encuentros sobre Informática y Derecho 2002-2003. Universidad de Comillas, Madrid, Facultad de Derecho, Instituto de Informática Jurídica, p.59-60

[100] *Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:*
a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; o
b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

[101] A. GARRIGA DOMÍNGUEZ, op. cit. 110

diversas razones exigen una protección máxima, habida cuenta de lo directamente comprometidas que se hallarían la dignidad y libertad de las personas por su uso ilegítimo, y que se desarrollan a continuación:

A. Informaciones que revelen la ideología, afiliación sindical, religión y creencias:

En el artículo mencionado se hace alusión al apartado 2 del artículo 16 de la Constitución Española, según el cual nadie podrá ser obligado a declarar sobre su ideología, religión y creencias. Han surgido algunas críticas entorno a la decisión del legislador de incluir el artículo 16 de la Constitución, "*cuando resultaba mucho más completo y pertinente haber tomado como punto de referencia el artículo 14 de la propia Constitución que previene cualquier actividad discriminatoria*"[102].

En oposición a esta crítica, Garriga Domínguez argumenta que *"si tomamos como referencia para la calificación de datos sensibles las expresas razones de prohibición de la discriminación del artículo 14 de la Constitución – nacimiento, raza, sexo, religión, opinión o cualquier otra circunstancia personal o social -, podríamos acabar concluyendo que cualquier información personal debería ser considerada como sensible".*

A lo expuesto es posible agregar que el artículo 14, en su último inciso se refiere a *"cualquier circunstancia personal o social",* esto también podría inducirnos a considerar sensible cualquier información personal que sirva para llevar a cabo un tratamiento desigual discriminatorio, prohibido por el texto constitucional. No obstante lo anterior, la referencia al artículo 14 de la Constitución de 1978, aporta una ventaja respecto del 16 y es su engarce directo con la noción de dignidad humana del artículo 10 del texto constitucional, porque en la discriminación existe también una negación del individuo de su condición plena de persona humana.

El reforzamiento de la protección de los datos relativos a ideología, afiliación sindical, religión y creencias que establece la ley en su artículo 7 consiste en las dos exigencias, por un lado, que

[102] A. E. PÉREZ LUÑO, *La tutela jurídica de los datos personales en España,* en la Toga, nº 131, Ilustre Colegio de Abogados de Sevilla, diciembre de 2001, p. 8

solo podrán ser objeto de tratamiento cuando el afectado preste su consentimiento de forma expresa y por escrito; y por otro que cuando se proceda a recabar el consentimiento del interesado, deberá advertírsele de su derecho a no prestarlo.

B. Los datos relativos al origen racial, a la salud y a la vida sexual:

Estos datos no podrán ser recogidos, tratados o cedidos salvo que el interesado consienta expresamente o cuando, por razones de interés general, lo disponga la ley. Es decir, se exige siempre el consentimiento del interesado.

Se recoge una tercera garantía específica para los datos sensibles en el artículo 7 de la LOPD, que consiste en la prohibición de crear ficheros con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.[103] Por lo tanto, esta tercera cautela pretende reforzar la protección de los dos grupos anteriores de datos sensibles, a excepción de las informaciones referentes a la salud.

Orozco Pardo[104], considera muy acertadamente que poco interés puede haber en el origen racial de las personas, si no es para discriminar y quebrar el principio de igualdad y, en cuanto a la vida sexual, difícilmente se puede entender tal interés.

C. Los datos sensibles relativos a la salud:

Reciben un tratamiento legal diferente en razón de su propia naturaleza. Son datos relativos a la salud cualquier información concerniente a la salud pasada, presente y futura, física o mental de un individuo. Es indiferente que se trate de una persona de buena o mala salud.

La regulación de los datos relativos a la salud del artículo 7 de la LOPD se complementa con lo dispuesto en el artículo octavo[105],

[103] Artículo 7.4 LOPD

[104] G. OROZCO PARDO, "*Consideraciones sobre los derechos de acceso y rectificación en el proyecto de ley orgánica de regulación de datos de carácter personal*", Informática y Derecho, nº 6-7 1994 p.231.

[105] La norma del artículo 8 de la LOPD se completa en la actualidad con lo previsto en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y

que autoriza a las instituciones sanitarias y a centros sanitarios, públicos y privados, y a los profesionales correspondientes a tratar los datos relativos a la salud de las personas que acudan a ellos o hayan de ser tratados en los mismos. En estos casos se procederá de acuerdo con lo previsto en la legislación sanitaria, estatal o autonómica.

Las condiciones para el tratamiento legítimo de los datos relativos a la salud vendrán establecidas en la legislación específica, en la cual además encontramos definidos los posibles intereses justificantes del tratamiento de dichos datos. Éste estará justificado, en la mayoría de los casos para proteger la salud del interesado, pero también podrán respaldarlo otras razones de interés general como puede ser la salud de la población en general o de terceras personas.

D. Los datos que hacen referencia a la comisión de infracciones penales o administrativas:

Estos datos sólo podrán figurar en los ficheros de las Administraciones públicas competentes en los supuestos en las normas reguladoras. Esta exigencia, es decir que la posibilidad de crear y mantener ficheros con esta clase de datos se limite en exclusiva a las Administraciones Públicas competentes no sólo responde al objetivo de garantizar la libertad informática del individuo, sino que está también relacionada con *"el objetivo de no frustrar los efectos regeneradores que atribuye a las sanciones el artículo 25 de la Constitución"*[106].

3. El derecho de información, previo al tratamiento:

El derecho de información previo al tratamiento de los datos de carácter personal es uno de los derechos básicos y principales contenidos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y constituye una de las facultades que configuran el derecho a la autodeterminación informativa, el derecho a ser

obligaciones en materia de información y documentación clínica; y por lo previsto en la Ley 14/1986, de 25 de abril, General de Sanidad, en cuanto no haya sido expresa o tácitamente derogada por la anterior.

[106] P. LUCAS MURILLO DE LA CUEVA, *Informática y protección de datos personales*. Cuadernos y Debates Nº 43, Centro de Estudios Constitucionales, Madrid, 1996 p. 72

informado se presenta como un requisito evidente e inicial, que nos permite verdaderamente controlar cómo, dónde y para qué tienen nuestros datos; pues como lo expresa el Tribunal Constitucional en su Sentencia 292/2000 en su fundamento jurídico octavo, *"el poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen y con qué fin"*. Este derecho se encuentra establecido en el artículo 5.1 de la LOPD[107], que recoge los supuestos que se expone a continuación:

a) Existencia de un fichero o tratamiento de datos de carácter personal:

Esta información resulta de suma importancia, ya que como apunta Aparicio Salom[108], de ella depende que se autorice la inclusión de los datos en el fichero, con independencia de la finalidad a que se destinen, de modo que en el caso de que se incumpla la obligación de informar sobre este aspecto, cabría la posibilidad de entender que no se ha consentido la principal de las situaciones de que depende el tratamiento leal de los datos.

b) Finalidad de la recogida de los datos:

Mediante esta información deberá comprender el interesado cuáles son los usos a los que se van a destinar los datos, tener un conocimiento claro de las actividades para las que van a servir. No

---

[107] *1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*
a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

[108] J. APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Navarra, 2000, p.90

obstante, en cuanto a este derecho, el concepto que utiliza la LOPD es de carácter abstracto, se refiere con ello a categorías genéricas de actividades o usos, de modo que deberán entenderse como tales la ejecución de un contrato en general o de algún tipo de actividad o producto concreto, el uso por terceros de la información, con acceso a la misma, mediante su cesión, en el caso de que se limite el responsable a la segmentación de la información y a prestar al publicista el servicio de emisión de la campaña entre las personas seleccionadas, etc.

c) Del carácter obligatorio o facultativo de su respuesta:

La Ley establece que se le informe al afectado acerca de la obligatoriedad de responder a las preguntas que se le realizan y las consecuencias de la obtención de de los datos o la negativa a facilitarlos. Resulta común que en el momento de solicitar los datos de carácter personal se soliciten más datos que los estrictamente necesarios para atender la finalidad para la que los datos resultan precisos. El motivo que suele justificar esta solicitud de información adicional es la existencia de otra finalidad, además de la aparente, para la que se precisan los datos adicionales. En consecuencia, mediante la exigencia de esta información, la Ley trata de garantizar que no se condicione, ni siquiera en apariencia, la celebración del contrato que motiva la relación entre el interesado y el responsable del tratamiento a la obtención del consentimiento para el tratamiento de más datos que los precisos.

d) Posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición:

La información a este respecto no debe limitarse sólo a la posibilidad de ejercer tales derechos, sino que deberá también comprender los medios y lugares en que puedan hacerse efectivos los mismos. De este apartado se desprende que el responsable del tratamiento, deberá dar a conocer al afectado que éste dispone, previamente al tratamiento de sus datos, de facultades que le permitirán ejercer sus derechos de acceso, rectificación, cancelación y oposición. En cualquier caso, esta información no resulta tan relevante como las mencionadas antes, puesto que la Ley establece la posibilidad de que pueda obviarse cuando se

deduzca claramente de la circunstancias en que se recaban los datos o la naturaleza de éstos, si bien parece que en este caso existe un error en el establecimiento de la excepción, ya que como lo expone Aparicio Salom[109], difícilmente podrá resultar evidente la posibilidad de ejercer estos derechos en atención a los datos o las circunstancias en que se recaban.

E) Identidad y domicilio del responsable del tratamiento:

La información sobre este aspecto tiene por objeto, fundamentalmente, que se conozca por parte del interesado quién es el responsable del tratamiento, a los efectos de poder mantener aquellas relaciones que considere oportunas con él, distintas de los derechos de acceso, rectificación y cancelación a que se hace referencia en el apartado anterior, y asimismo, que conozca la identidad de la empresa o persona que lleva a cabo el tratamiento de los datos, a los efectos de no confundir al responsable del tratamiento con un nombre comercial o marca.

F) Destinatarios de la información:

Finalmente, es menester hacer referencia al deber de información sobre el destinatario de la información establecido en el apartado a) del artículo 5.1.Esta información no está, evidentemente, referida a las cesiones que se pretendan realizar, sino al supuesto de que la obtención de los datos no se esté realizando directamente por el responsable del tratamiento, sino por un tercero a su encargo.

En este caso, por lo tanto, no debe entenderse incluido entre los supuestos que se han denominado comunes del deber de información, sino sólo referido al caso de obtención de la información directamente del interesado.

4. El consentimiento del afectado:

Este derecho se encuentra establecido en el artículo 6 de la LOPD que dispone: *"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa".*

[109] J. APARICIO SALOM, op. cit. p. 92

A su vez, el artículo 3.h) de la Ley Orgánica 15/1999 define al consentimiento del interesado como *"toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen",* de lo cual se desprende la necesaria concurrencia de los cuatro requisitos enumerados en dicho precepto, para que el consentimiento pueda ser considerado conforme a derecho.

Es importante a la luz de este derecho, realizar un análisis de los requisitos mencionados según se conciben cada uno de ellos:

> ***a) Libre:*** Lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.[110]
>
> ***b) Específico***: es decir referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.2 de la Ley Orgánica 15/1999.[111]
>
> ***c) Informado:*** es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la Ley Orgánica impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.
>
> ***d) Inequívoco:*** lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado, siendo preciso que exista expresamente

[110] El artículo 1262 del Código Civil Español dispone que: "*El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato. Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta. En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación.*" Este artículo ha sido modificado por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE núm. 166, de 12/7/2002, p. 25388-25403).

[111] "*Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos*".

una acción u omisión que implique la existencia del consentimiento.

De lo que se ha indicado se desprende que de las características del consentimiento no se infiere necesariamente su carácter expreso en todo caso, razón por la cual en aquellos supuestos en que el legislador ha pretendido que el consentimiento deba revestir ese carácter, lo ha indicado expresamente; así sucede en el caso de tratamiento de datos especialmente protegidos indicando el artículo 7.2 la necesidad de consentimiento expreso y escrito para el tratamiento de los datos de ideología, religión, creencias y afiliación sindical, y el artículo 7.3 la necesidad de consentimiento expreso aunque no necesariamente escrito para el tratamiento de los datos relacionados con la salud, el origen racial y la vida sexual.

Por tanto, el consentimiento podrá ser tácito, en el tratamiento de datos que no sean especialmente protegidos[112], si bien para que ese consentimiento tácito pueda ser considerado inequívoco será preciso otorgar al afectado un plazo prudencial para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento implica un consentimiento al mismo.

5. El derecho de oposición al tratamiento:

El artículo 6.4 de la LOPD regula el derecho de oposición al tratamiento de la siguientes manera *"en los casos en que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos del afectado"*.

La norma compensa de esta manera al afectado, en aquellos casos en los cuales no sea necesario solicitar su consentimiento para el tratamiento de sus datos personales y se destaca y valora su inclusión en la LOPD, teniendo en cuenta que este derecho supone una novedad ya pues al revisar la legislación anterior, es posible

[112] Artículo 7.2 y 7.3 de la Ley Orgánica 15/1999

notar que la LORTAD no había contemplado con carácter general la posibilidad de oposición al tratamiento de datos[113].

Al realizar un análisis comparativo de la LOPD con la Directiva 95/46/CE, es posible notar que ésta no sigue fielmente en sus disposiciones la regulación del derecho de oposición que se ha introducido en la normativa comunitaria. En efecto, el derecho de oposición en el ámbito comunitario alcanza un significado diferente, por cuanto el artículo 14 de la citada Directiva, concede este derecho únicamente frente a los tratamientos destinados a la prospección y a los supuestos contemplados en el artículo 7 apartados e) y f) de la Directiva 95/46/CE[114]; en tanto que, por el contrario, la LOPD contempla un derecho de oposición general, reconocido para todos aquellos supuestos en los que no se necesario el consentimiento, a no ser que una ley excluya este derecho. Asimismo, la LOPD exige en todo caso que la oposición del interesado se realice por motivos fundados y legítimos, relativos a una concreta situación personal, lo que en principio parece más ajustado que lo dispuesto en la norma comunitaria, la cual facilita el derecho de oposición "en cualquier tiempo, por razones legítimas propias de su situación particular"[115].

Algunos autores[116] critican también el escaso acierto del legislador a propósito de la ubicación sistemática en la Ley del derecho de oposición; en verdad, en lugar de introducirse en el ámbito del Título III relativo a los derechos de las personas, el

[113] Aunque el artículo 29 de la derogada LORTAD, en relación con los ficheros de publicidad reconocía a los interesados el derecho a darse de baja de forma inmediata del fichero, cancelándose las informaciones personales que sobre ellos figurasen en el fichero, a su simple solicitud, esto es, sin especiales requisitos que justifiquen la adopción de esta medida por el interesado. Luego se reconocía la oposición al tratamiento para unos ficheros con fines concretos de publicidad, pero no se extendía el reconocimiento de este derecho para otros tratamientos, con carácter general.

[114] Artículo 7

"Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva".

[115] Artículo 14, Directica 95/46/CE

[116] HERRÁN ORTÍZ, op.cit. 60

derecho de oposición se inserta dentro del Título II correspondiente a las previsiones comunitarias, que expresamente contemplan este derecho como uno más de los derechos reconocidos al afectado.

En el artículo 17 de la LOPD completa la regulación del derecho de oposición, cuyo ejercicio será gratuito. De todo lo expuesto se desprende la importancia que en la actualidad alcanza el reconocimiento al interesado de este derecho, que actúa como una medida preventiva que puede facilitar al interesado una actuación previa a cualquier daño o perjuicio derivado del tratamiento no deseado de sus datos personales, bien es verdad que para poder oponerse al tratamiento de sus datos personales deben existir motivos fundados y legítimos. En definitiva, el legislador intenta garantizar a través del derecho de oposición una facultad de actuación al interesado que por motivos fundados no desea que sus datos personales sean objeto de tratamiento.

6. El derecho de consulta:

La Ley 15/1999 Orgánica de Protección de Datos, reconoce con carácter general el derecho de consulta, según el cual *"cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita"*[117].

Es posible observar que la norma habla de un derecho general de consulta principalmente por dos circunstancias: en primer lugar, se reconoce la posibilidad de ejercitar dicho derecho a "cualquier persona", sin que sea requisito preciso que se trate de la persona afectada o interesada al efecto; y en segundo lugar, se justifica la amplia legitimación para el ejercicio de este derecho por cuanto que la información a la que se accede no afecta a derechos ni libertades individuales de las personas. En efecto, se podrá obtener información sobre "la existencia de tratamiento de datos, sus fines y la identidad del responsable del tratamiento", sin que en ningún caso, se facilite información personal de los afectados por dichos

[117] Artículo 14 LOPD

tratamientos.[118] Esto se debe a que la Agencia Española de Protección de Datos no dispone de datos de los ciudadanos, sino de los ficheros inscriptos en el Registro General de Protección de Datos y de los responsables de éstos ficheros, así como de las direcciones de éstos a fin de que las personas que consideren que se encuentran incluidas en estos ficheros puedan ejercer su derecho de acceso previsto en la Ley.

Es el afectado titular de éste derecho quien deberá ejercerlo, pues es a él a quien le corresponde la iniciativa y quien tiene reconocida la facultad de solicitar al Registro General de Protección de Datos información sobre los tratamientos de datos personales, con el propósito de ejercitar posteriormente el derecho de acceso a la información. Por ello, la consulta al citado Registro constituye un complemento necesario para el ejercicio del derecho de acceso; sólo conociendo la existencia del tratamiento de datos, es decir, de un fichero automatizado o no que contenga datos de carácter personal, su finalidad y la identidad de su responsable, será posible garantizar el ejercicio del derecho de acceso al afectado.

Cabe destacar la importancia del carácter gratuito y público de éste derecho, lo que sin duda contribuye a animar a los interesados al ejercicio del mismo, al tiempo que evita la introducción de un elemento limitativo del ejercicio práctico del mismo[119]. Ello constituye una importante facultad instrumental, que facilita el ejercicio del derecho de acceso a los afectados.[120]

Otra circunstancia que debe significarse es la relativa a la consulta de los ficheros o tratamientos convencionales que la LOPD contempla en la Disposición adicional primera cuando establece que *"su adecuación a la presente Ley Orgánica, y la obligación*

[118] A. I. HERRÁN ORTÍZ, op. cit., p. 61

[119] Con respecto al carácter gratuito de este derecho, es importante destacar que el Convenio 108 del Consejo de Europa nada prevé a propósito de la necesidad de un acceso gratuito y público a los tratamientos de datos personales (vid. Artículo 8 a), la Directiva 95/46/CE en su artículo 12 a) se refiere al derecho a confirmar la existencia o inexistencia de tratamientos de datos que conciernen al interesado "*sin retrasos ni gastos excesivos*", luego contempla la posibilidad de que dicho acceso no sea gratuito, si bien queda claro que nunca la contraprestación podrá significar en la práctica una limitación para el ejercicio del acceso.

[120] En el capítulo IV del presente trabajo, el cual trata acerca de la estructura de la AEPD, se expondrá detalladamente la información referida a la forma en que debe ejercerse el derecho de consulta ante el Registro General de Protección.

prevista en el párrafo anterior- la de inscripción de los ficheros en el Registro General de Protección de Datos – deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados". Luego, los tratamientos manuales que habían permanecido al margen de la regulación en el ámbito de la LORTAD (vid. Disposición Final Segunda), a partir de la entrada en vigor de la LOPD deberán también regularizarse y adaptarse a las disposiciones y exigencias de la nueva regulación de protección de datos personales.[121]

7. Los derechos de acceso, rectificación y cancelación:

A. Derecho de Acceso:

El derecho de acceso se encuentra reconocido en el artículo 15.1 de la LOPD al interesado y comprende el *"derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos".*

Este es un derecho personalísimo, lo cual significa que deberá ser ejercitado por el propio interesado, frente al responsable del fichero; para ello deberá acreditar su identidad[122] frente al responsable del fichero. Ello no obstante, el afectado podrá actuar por medio de su representante legal cuando aquél se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal del derecho.[123]

Esta limitación respecto de su ejercicio supone que sólo el interesado puede ejercerlo, de modo que un tercero no puede

[121] Cabe recordar que el artículo 3 de la Directiva 95/46/CE expresamente amplía la aplicación del texto comunitario a los tratamientos no automatizados de datos personales por lo que la adaptación de la normativa española a la Directiva comunitaria en este punto era necesaria para avanzar en la protección de los datos personales. Tal y como se afirma en el Considerando 27 de la Directiva 95/46/CE, el alcance de la protección a las personas en este ámbito no debe depender de las técnicas utilizadas en el tratamiento de datos.

[122] Con carácter general, se ha venido exigiendo en la práctica por parte de los responsables de los tratamientos, en atención a la Instrucción 1/1998, que a la solicitud del acceso se acompañe una copia del Documento Nacional de Identidad o algún otro documento identificativo oficial, para garantizar que el acceso se está ejerciendo por la persona interesada y no por un tercero.

[123] Artículo 1 Instrucción 1/1998 de la Agencia de Protección de datos, de 19 de enero

acceder a los datos de otra persona. Sin embargo, el tenor literal de esta regla limita la posibilidad de que se ejerzan los derechos por medio de una representación voluntaria.

Como en el caso del derecho de consulta, también el derecho de acceso se configura en la LOPD como derecho gratuito[124], lo que garantiza que el carácter remuneratorio del ejercicio de estos derechos no dificulte o imposibilite el ejercicio de un derecho que tanta significación alcanza en el contenido esencial del derecho a la protección de datos personales.

Los procedimientos previstos para el ejercicio del acceso a la información pueden ser *"la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos",* según el Artículo 15.2 de la LOPD. También han de considerarse otros posibles medios de acceso a la información personal, habida cuenta que el Real Decreto 1332/94, vigente en lo que no contradiga la LOPD, en su artículo 12.2 establece que podrá realizarse también el acceso mediante *"cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del fichero"*.

En todo caso, la información, cualquiera que sea el soporte en que se facilite, se dará en forma legible e inteligible y comprenderá los datos de base del interesado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron. En el caso de que los datos provengan de fuentes diversas deberán especificarse las

[124] Sorprende desde luego que el legislador español no haya seguido en este punto lo dispuesto en el Convenio 108 del Consejo de Europa – art. 8 b) – ni lo contemplado por el artículo 12 de la Directiva 95/46/CE, que preveían el acceso "sin gastos excesivos", con lo que facilitaban la regulación de una acceso remuneratorio; sin embargo, el texto español ha optado por excluir los gastos del acceso, en un intento por garantizar el ejercicio de este derecho, de suerte que la imposición de una remuneración no suponga una disuasión para el interesado en el ejercicio.

mismas identificando la información que proviene de cada una de ellas.[125]

Según aclara la Instrucción 1/1998, la Ley configura los derechos de acceso, rectificación y cancelación como derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

El Real Decreto1332/94, establece que en el plazo máximo de un mes, a contar desde la recepción de la solicitud, el responsable del tratamiento deberá resolver sobre la petición de acceso, bien entendido que en el supuesto de que transcurra dicho plazo sin que se haya contestado la solicitud se entenderá que ésta ha sido desestimada; si fuere estimada el ejercicio del acceso deberá ser efectivo en el plazo de los diez días siguientes a la notificación de la resolución estimatoria[126].

La Ley sólo permite la denegación del derecho de acceso en el caso de que se ejerza antes de que hayan transcurrido doce meses desde la última vez que se solicitó y no se acredite por el interesado la concurrencia de un interés legítimo que justifique el incumplimiento de dicho plazo mínimo.[127]

Por último, la Ley garantiza el cumplimiento de la solicitud de acceso por el responsable del fichero, cuando dispone que la obstaculización del derecho de acceso y la negativa a facilitar la información que se ha solicitado, constituye una infracción grave, según el artículo 44.3 e) de la LOPD; y según el artículo 44.4 h) de la misma Ley, la infracción será muy grave cuando de forma sistemática o continuada se impida el ejercicio de acceso.

B. Los derechos rectificación y cancelación:

Una vez que el interesado ha ejercitado el derecho de acceso el interesado puede encontrar que los datos personales objeto de tratamiento son incompletos o erróneos, o tal vez compruebe que su tratamiento es ilícito. Es entonces cuando el interesado puede

[125] Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación., Norma Segunda, inciso 6.
[126] Artículo 12.3 Real Decreto 1332/1994
[127] Artículo 15.3 LOPD

exigir la rectificación, la cancelación o el bloqueo de los datos personales objeto del tratamiento.

Los derechos de rectificación y cancelación se encuentran establecidos en el artículo 16 de la LOPD, el cual dispone *"serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos"*[128]. Aunque estén regulados en forma conjunta en el mencionado artículo, se trata de dos derechos diferentes. Por un lado, el interesado tiene derecho a que los datos que figuren de manera inexacta o errónea en un fichero sean corregidos e integrados y, por otro, la facultad de eliminar de un fichero aquellos datos de carácter personal *"que no deban figurar en él, ya sea porque nunca debieron ser registrados, ya sea porque habiéndose recogido legalmente, diversas causas exigen su supresión"*[129]. Es decir, los datos serán rectificados, o en su caso cancelados, cuando sean incompletos, erróneos, excesivos, no adecuados, se hayan obtenido de manera desleal o engañosa, sin el consentimiento del afectado cuando éste sea imprescindible, o se haya vulnerado algún otro precepto legal en su recogida o tratamiento[130].

Los derechos de rectificación y cancelación suponen para el responsable del tratamiento, no sólo la obligación de rectificar o cancelar los datos personales, sino además, en caso de comunicación, el deber de notificar a quien se haya comunicado los datos, la rectificación o cancelación efectuada sobre los datos cedidos. El artículo 16.4 de la LOPD obliga al cesionario de los datos a proceder también a la cancelación de los datos, en los casos anteriores y cuando aún mantenga su tratamiento, aunque lo lógico sería entender que cuando el responsable del tratamiento originario haya rectificado los datos personales y se lo comunique al responsable cesionario, éste procederá igualmente a rectificarlos.

El procedimiento para el ejercicio y la atención de los derechos de rectificación y cancelación se regula en la el Real Decreto1332/94 y en la Instrucción 1/1998 de la Agencia Española

[128] Artículo 16.2 LOPD
[129] P. LUCAS MURILLO DE LA CUEVA, *Informática y protección de datos personales*, op. cit. p.79
[130] A. GARRIGA DOMÍNGUEZ, op.cit. p. 132

de Protección de Datos. Al igual que se establece para el derecho al acceso, los derechos de rectificación y cancelación son personalísimos, exigiéndose para su ejercicio las mismas formalidades de identificación y apoderamiento que respecto del derecho de acceso, que se analizan en el apartado anterior.

El responsable del fichero deberá hacer efectivo el derecho de rectificación del afectado dentro del plazo de diez días[131] siguientes al de la recepción de la solicitud y, en idéntico plazo, se notificará al cesionario la rectificación operada. Por la rectificación o la cancelación de los datos no se le podrá exigir al interesado contraprestación alguna de acuerdo con el artículo 17.2 de la LOPD, pero además, porque el artículo 4 de la mencionada norma establece para los responsables de los tratamientos, la carga de mantenerlos en consonancia con la situación real del titular de los datos, es decir, *"los datos serán exactos y puestos al día de forma que respondan con la veracidad a la situación actual del afectado"*[132], *"si los datos de carácter personal registrados resultaran inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados"*[133] y *"serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recabados o registrados"*[134].

Resulta especialmente significativa la consecuencia material que la LOPD en su artículo 16.3 contempla para la cancelación de datos personales, cuando establece que *"la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, jueces y tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el*

[131] El plazo para proceder a la rectificación o cancelación de los datos personales es de diez días según se explicita en el artículo 16.2 de la LOPD; también hace referencia a esta cuestión el artículo 15.2 del Real Decreto 1332/1994, si bien el plazo contemplado en esta norma es de cinco días a contar desde la recepción de la solicitud. Realizando la contraposición de ambas normas, y a tenor de lo previsto en la Disposición Transitoria Tercera de la Ley 15/1999, habrá que estar al plazo fijado en la LOPD ya que el Real Decreto 1332/1994 continuará en vigor "en cuanto no se oponga a la presente Ley" y como en este caso existe notoria oposición con la LOPD, prima ésta última, quedando vigente el plazo de diez días.

[132] Artículo 4.3 LOPD

[133] Artículo 4.4 LOPD

[134] Artículo 4.5 LOPD

plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión".

De la norma parece desprenderse una equiparación efectiva y práctica entre cancelación y bloqueo de los datos personales, cuando puedan derivarse responsabilidades del tratamiento de los datos, bien entendido que éstos únicamente se conservarán a los efectos de su consulta por las autoridades judiciales que correspondan para la delimitación de tales responsabilidades.

El límite entre la cancelación que conlleva la destrucción de los datos y la que únicamente provoca el bloqueo de la información se encuentra en la forma de recogida y tratamiento de los datos personales, esto es, cuando la obtención y tratamiento de los datos personales se realice por medios ilícitos o fraudulentos[135] no será posible proceder a la cancelación a través del simple bloqueo de los datos, sino que en cualquier caso deberá destruirse la información.

También es necesario mencionar otra excepción que contempla la LOPD según la cual "los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado"[136]. Pero además de ésta obligación general de conservar en tales supuestos, la LOPD prevé especiales plazos de conservación de los datos personales; así, por ejemplo, destaca el plazo de conservación establecido en el artículo 29 de la LOPD en relación con los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito, según el cual *"sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos"*.

Sólo los tratamientos de titularidad pública están amparados por algunas excepciones al derecho de acceso, rectificación y cancelación, en el caso de que exista un interés público en mantener secreto el contenido del tratamiento, por razones de

[135] Instrucción 1/1998, Norma Tercera inciso 9
[136] Artículo 16.5 LOPD

interés y orden público, lo cual se encuentra establecido en el artículo 23 de la LOPD[137] y con respecto a ello también se pronuncia la norma segunda inciso 5 de la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

8. El derecho a indemnización:

Este derecho se encuentra regulado en el artículo 19 de la LOPD, el cual dispone que los interesados que, como consecuencia del incumplimiento de lo dispuesto en la Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

Si se tratara de ficheros públicos, la responsabilidad se exigirá de acuerdo con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas; si son de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

Recapitulando, se hace depender el régimen de responsabilidad civil del incumplimiento de las normas por el responsable del tratamiento, y no se vincula el deber de reparar el daño con la existencia; por ello, no será suficiente la relación de causalidad entre el tratamiento de datos y el perjuicio, se precisa además que pueda imputarse al responsable del tratamiento un incumplimiento del que se derive el daño. Así lo ha interpretado

[137] *1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.*
2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.
3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del Organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones Tributarias Autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Grimalt Servera[138], al considerar que se excluye la existencia de una responsabilidad objetiva absoluta, porque se configura un régimen de imputación a partir del incumplimiento de los deberes u obligaciones legales del responsable del tratamiento; por ello, si ha existido incumplimiento, y de éste se deriva un perjuicio para el afectado tendrá derecho a indemnización, con independencia de la concurrencia o no de culpa.

Herrán Ortiz[139], al analizar este tema, manifiesta que debe reprocharse al legislador español que sean numerosos e importantes los silencios legales en la materia de responsabilidad por el tratamiento de datos; ya que así quedan sin respuesta en la LOPD cuestiones como los perjuicios a que se extiende la indemnización, la forma en que han de valorarse los daños y las excepciones a la responsabilidad legal.

En primer lugar, de excluir el daño moral, poco será lo que quede para indemnizar; surge también la duda respecto a la valoración misma de ese daño, a la que la Ley tampoco ofrece respuesta. Ahora bien, en cada caso tendrán que valorarse aspectos tales como la naturaleza de los derechos implicados, la difusión concedida a tales datos y el lucro o beneficio obtenido con el tratamiento.

Por otro lado, Ortí Vallejo[140], expone otro punto de vista, según el cual no ha de admitirse judicialmente con carácter general el reconocimiento de indemnizaciones por la utilización indebida de los medios informáticos, ya que ello impediría una deseable despatrimonialización de los derechos fundamentales.

Con respecto a esa teoría, es menester admitir que constituye un error enfrentar la despatrimonialización de los derechos fundamentales al reconocimiento de un legítimo derecho a recibir indemnización por los daños y perjuicios que a los bienes y derechos personales haya causado el tratamiento de datos

[138] P. GRIMALT SERVERA, *La responsabilidad civil en el tratamiento de automatizado de datos personales*, Colección Estudios de Derecho Privado, núm 8, Granada 1999 p. 254-255
[139] A. HERRÁN ORTÍZ, *El derecho a la protección de datos personales en la sociedad de la información.* Universidad de Deusto. Bilbao.2003 p. 73
[140] A. ORTÍ VALLEJO, *Derecho a la intimidad e informática. Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada*, Granada, Comaraes 1994, p 168-169

personales. Sin embargo, no puede desconocerse el derecho de indemnización del daño moral porque el interesado tenga reconocidos otros derechos de defensa frente al tratamiento de sus datos, como el derecho de oposición, rectificación o cancelación de los datos. Se trata de derechos diferentes, unos intentan prevenir utilizaciones ilícitas de los datos, y el otro pretende resarcir un incumplimiento del que sea ha derivado un perjuicio para el interesado.

CAPÍTULO IV
GARANTÍAS DE LOS DERECHOS DEL INTERESADO

I -Ámbito Español:

Al iniciar el estudio de las garantías de los derechos del interesado en la protección de sus datos personales a nivel español, se debe distinguir dos modalidades, pues existen tanto garantías institucionales como jurisdiccionales, que posibilitan la protección del derecho establecido en el artículo 18.4 de la Constitución Española. Primeramente analizaremos la labor de la Agencia Española de Protección de Datos, institución que tiene a su cargo la labor de velar por el cumplimiento de la Ley 15/1999 de protección de datos, y las Agencias Autonómicas que también constituyen una garantía institucional al servicio del ciudadano; para luego emprender el estudio de las garantías jurisdiccionales existentes en el ordenamiento jurídico español a través de las cuales el ciudadano puede defender su derecho a la autodeterminación informativa.

1. Garantías Institucionales:

A. La Agencia Española de Protección de Datos:

El derecho a la autodeterminación informativa tiene, además de las garantías comunes a todos los derechos fundamentales, una garantía específica introducida por la LORTAD: La Agencia Española de Protección de Datos (en adelante AEPD). Esta garantía

"nace y existe para hacer efectivo el derecho a la autodeterminación informativa, libertad informática o derecho a la intimidad". [141]

En primer lugar se tuvo en cuenta lo establecido en la normativa internacional sobre la materia que vincula a España. La primera de las normas que hizo referencia a la existencia de una autoridad de control fue el Convenio 108[142], aprobado en el seno de Consejo de Europa, aunque no definía los criterios ni la pautas que debían inspirar la actuación y las funciones del citado órgano en el ámbito nacional. Posteriormente, el Acuerdo de Schengen también exigió que cada Parte contratante designara a una autoridad de control independiente encargada de controlar el fichero de la parte nacional del sistema de Schengen[143]. Por último, la Directiva 95/46/CE estableció los criterios que debían regir la creación y organización de estas autoridades en los países miembros[144].

En segundo lugar, el legislador español, de acuerdo con las normas antes mencionadas, entendió que, debido a las amplias posibilidades de lesión que ofrece actualmente la informática, era preciso crear un órgano independiente, especializado en la materia, que respondiera de forma rápida y que actuara de forma preventiva. Esta problemática fue abordada por la derogada LORTAD y en la actual LOPD, al plantearse la disyuntiva de cómo podía efectuarse, con máxima garantía posible, la protección de los derechos previstos en la legislación vigente, compaginando esta garantía con la máxima eficacia[145].

---

[141] P. LUCAS MURILLO DE LA CUEVA, "*Las funciones de la Agencia de Protección de Datos"*, en Jornadas sobre el Derecho Español de la Protección de Datos Personales, Agencia de Protección de Datos, Madrid 1996, p.265. en A. GARRIGA DOMÍNGUEZ, *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid 2004. p.183

[142] El artículo 13 del Convenio 108, que regula la colaboración entre grupos, prevé la obligación de designar una o más autoridades, se entiende que de control, cuyos nombres serán comunicados al Secretario General del Consejo de Europa. Pero estas autoridades se nombran con la única finalidad de que esté enlazado el sistema de comunicación y asistencia entre las partes contratantes de la Convención, lo que si bien no los convierte en órganos de control puros suponen un germen de esta actividad.

[143] Artículos 114.1 y 128.1 Acuerdo Schengen, ratificado por Instrumento de 23 de julio de 1993.

[144] M. ARENAS, *El derecho fundamental a la protección de datos personales en Europa*, Agencia Española de Protección de Datos, Tirant lo Blanch, Valencia, 2006. p. 574.

[145] G. FREIXAS GUTIÉRREZ, *La protección de datos de carácter personal en el derecho español*, Bosh, Barcelona. 2001 p.286

En un principio se planteó la posibilidad de que fuera el Defensor del Pueblo[146] el encargado de la protección de datos personales, aunque esta idea fue desechada por la posible desvirtuación que se produciría de la institución del Defensor del Pueblo, y se decidió crear de esta manera un organismo específico, la Agencia de Protección de Datos. Con respecto a ello se ha pronunciado el Tribunal Constitucional, y ha afirmado *"la creación de dicho ente y las funciones atribuidas al mismo permiten garantizar el ejercicio por los ciudadanos del haz de facultades que integran el contenido del derecho fundamental a la protección de datos"*[147].

a) Naturaleza y régimen jurídico:

Como ya se había mencionado anteriormente, la Agencia de Protección de Datos fue creada por la LORTAD, así es posible apreciar los siguiente en su exposición de motivos: *"Para asegurar la máxima eficacia de sus disposiciones, la Ley encomienda el control de su aplicación a un órgano independiente, al que atribuye el estatuto de Ente público en los términos del artículo 6.5 de la Ley General Presupuestaria. A tal efecto, la Ley configura un órgano especializado, denominado Agencia de Protección de Datos, a cuyo frente sitúa un Director"*. Consecuentemente, en su artículo 34.2 la derogada LORTAD disponía que *"La Agencia de Protección de Datos es un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones"*.

Por otro lado, la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en su artículo 35.1 establece que *"La Agencia Española de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena*

[146] Teniendo en cuenta que la Ley 3/1981, de 6 de abril del Defensor del Pueblo, le atribuye como funciones la defensa de los derechos comprendidos en el Título I de la Constitución. Así también lo hace el artículo 54 de la Constitución Española. Pero el problema se plantea en los ficheros privados porque si bien podrá supervisar la actividad de la Administración, su actividad se reduce a esta parcela y no puede actuar en la esfera privada con lo que el control de estos ficheros hubiese requerido la creación de una figura paralela.

[147] Sentencia Nº 254/ y 290/2000.

independencia de las Administraciones Públicas en el ejercicio de sus funciones…". El artículo 36.2 de la LOPD también hace alusión a la independencia de este órgano al disponer que *"El Director ejercerá sus funciones con plena independencia y objetividad, y no estará sujeto a instrucción alguna en el desempeño de aquéllas".*

El Estatuto de la AEPD, establece a su vez, en su artículo 1.2 que *"La Agencia de Protección de Datos actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia."*

Si bien es cierto que la independencia de la AEPD, se encuentra acabadamente prevista en la normativa más arriba mencionada, es preciso determinar el verdadero grado de independencia de la institución que nos ocupa. Los cuestionamientos surgen alrededor de dos elementos fundamentales, en primer lugar con respecto al elemento personal y en segundo lugar al elemento relacional.

En lo que respecta a la primera cuestión, el elemento personal supone el reconocimiento de unas garantías especiales para el nombramiento y permanencia de los cargos directivos. El Director de la Agencia es nombrado por el Gobierno de entre los nueve miembros del Consejo Consultivo. Este último órgano está formado por nueve miembros de variada procedencia, como se verá en el apartado que lo desarrolla más abajo. Debido a esta variedad de procedencia se hace difícil identificar lazos comunes que permitieran alianzas estables de sus miembros y, por otro, la ausencia de intereses comunes puede propiciar, según manifiesta López Ramón, *"el dominio de los intereses gubernamentales, en la designación y ceses de los miembros del Consejo Consultivo"*[148].

Otra opinión digna de mencionar es la que sostiene acertadamente Garriga Domínguez, quien manifiesta que uno de los aspectos más criticables de la regulación legal de la Agencia, constituye el hecho de que el nombramiento del Director se haga

[148] F. LÓPEZ RAMÓN, *La Agencia de Protección de Datos como Administración independiente*, en Jornadas sobre el Derecho Español de la Protección de Datos Personales, Agencia de Protección de Datos, Madrid, 1996, p. 255. en A. GARRIGA DOMÍNGUEZ, *Tratamiento de datos personales y derechos fundamentales*, op. cit. p.185

por el Gobierno y no por el Parlamento. Este es el mismo punto de vista sostenido por Pérez Luño[149] quien lo ha criticado reconociéndolo como *"uno de los aspectos más negativos e insatisfactorios"*, que hace que se planteen serias dudas acerca de la pretendida independencia de la AEPD.

Por otro lado, Heredero Higueras sostiene que el hecho de que la designación del Director se haga por el Gobierno es irrelevante desde este punto de vista, ya que, en su opinión, la designación parlamentaria en sí misma también *"puede acarrear un riesgo de politización, en la medida en que la elección de su titular o titulares pueda estar mediatizada por la correlación de las fuerzas políticas"*[150].

La AEPD cuenta con amplias posibilidades de relación con otras organizaciones u organismos. Puede establecer relaciones con los distintos órganos de las Administraciones Públicas en el ejercicio de sus competencias; con otros organismos internacionales y de la Unión Europea, en materia de cooperación internacional, con los organismos autonómicos competentes en esta materia. Por otro lado, lo que resulta criticable por la doctrina, son las relaciones de control y cooperación con las Cortes a través de la presentación anual de una Memoria, aunque indirectamente a través del Ministerio de Justicia.

Algunos autores, como Pérez Luño, consideran que el hecho de que el Director de la Agencia deba presentar su informe anual ante el Ministro de Justicia, condiciona de manera grave la credibilidad y neutralidad de esa institución, y del Director *"que aparece como un mero delegado gubernativo para la informática"*[151].

Con respecto al punto de vista financiero, cabe agregar que los recursos económicos de la Agencia se nutren principalmente de las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales. Sin embargo, a ella corresponde la elaboración y aprobación del anteproyecto de su presupuesto

[149] A. E. PÉREZ LUÑO, *Derechos Humanos, Estado de Derecho y Constitución*, octava edición, Tecnos, Madrid, 2003, p. 372

[150] M. HEREDERO HIGUERAS, La Agencia de Protección de Datos, Informática y Derecho, Nº 6-7, UNED, Mérida, 1994, p. 326

[151] A. E. PÉREZ LUÑO, *Manual de Informática y Derecho,* Ariel, Barcelona, 1996, p. 56

anual, que deberá remitir al Gobierno para su incorporación de manera separada en los Presupuestos Generales del Estado. Por otro lado, la exterioridad y por tanto independencia de la Agencia respecto de la estructura de la Administración, *"se refleja en la ausencia del control de fiscalización de la Intervención General del Estado",* aunque ello no exime a la Agencia del control del Tribunal de Cuentas.[152]

Teniendo en cuenta lo expuesto más arriba, es posible concluir que, si bien es cierto, la AEPD supera ciertos parámetros de independencia, especialmente en lo que se refiere al punto de vista funcional, normativo y financiero, es importante reconocer que el nombramiento y cese del Director depende del Gobierno y que la Memoria se presenta ante el Ministro de Justicia y no ante las Cámaras. Estas dos últimas circunstancias condicionan también la independencia de la institución, por lo que hubiese sido deseable que el legislador hubiera subsanado en la LOPD estos aspectos específicos.

El artículo 79 de la Ley 62/2003[153], de 30 de diciembre, de medidas fiscales, administrativas y del orden social, publicada el día 31 de diciembre de 2003, ha modificado el nombre de la Agencia de Protección de Datos, por lo que a partir del día 1º de enero de 2004, ha pasado a denominarse Agencia Española de Protección de Datos.

Por su parte el Real Decreto 428/1993, de 26 de marzo, que aprueba el Estatuto de la AEPD, que continúa vigente en tanto no sea aprobado otro nuevo, completa la descripción de la naturaleza jurídica que realiza el citado art. 35 de la LOPD, señalando en su art. 1 que se trata de un ente público de los previstos en el art. 6.5 del Real Decreto Legislativo 1091/1988, de 23 de septiembre, que aprueba el Texto Refundido de la Ley General Presupuestaria. Este precepto fue derogado por la Ley 6/1997, de 14 de abril, de

[152] A. GARRIGA DOMÍNGUEZ, *Tratamiento de datos personales y derechos fundamentales*, op. cit. p.188

[153] Artículo 79. Agencia Española de Protección de Datos: "*La Agencia de Protección de Datos pasa a denominarse Agencia Española de Protección de Datos. Las referencias a la Agencia de Protección de Datos realizadas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como en las normas a las que se refiere su disposición transitoria tercera y cualesquiera otras que se encuentren en vigor deberán entenderse realizadas a la Agencia Española de Protección de Datos*".

Organización y Funcionamiento de la Administración General del Estado que, sin embargo, establece en su disposición adicional décima el régimen jurídico de determinados entes públicos, entre los que se encuentra la AEPD.[154]

b) Estructura y Funciones:

Desde su creación, la AEPD ha venido desempeñando importantes funciones que tiene encomendadas a fin de garantizar el derecho fundamental a la protección de datos personales. El desarrollo de estas funciones implica una serie de actividades que, en los últimos años, se han visto incrementadas de una forma muy significativa[155].

Por un lado, la Agencia dispone de significativas facultades normativas en el régimen de aplicación y de desarrollo de la legislación de protección de datos, informando los proyectos de disposiciones generales que desarrollen esta legislación. Los artículos 37 c) de la LOPD[156] y 5 apartados c) y d) del Estatuto[157] reconocen a la Agencia potestad normativa propia, mediante instrucciones y recomendaciones con la finalidad de adecuar los tratamientos automatizados a los principios de la Ley.

Por otro lado, el artículo 37 de la LOPD confía a la AEPD otras funciones que se refieren al cumplimiento de la legislación sobre protección de datos, a la adecuación de los tratamientos a los principios de la ley y al informe preceptivo de los proyectos de disposiciones generales que desarrollen el contenido de la LOPD. El Estatuto de la AEPD, detalla las funciones de la Agencia en su capítulo II, distinguiendo entre las referentes a las relaciones con los afectados, las de cooperación en la elaboración y aplicación de las normas, las relativas a los ficheros estadísticos, la publicidad de los ficheros, la elaboración de una memoria anual y las relaciones internacionales. Por lo que se refiere a las relaciones con los

[154] Memoria de la Agencia Española de Protección de Datos, Año 2005, p. 29
[155] Memoria de la Agencia Española de Protección de Datos, Año 2005, p. 18
[156] Artículo 37 *c) Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.*
[157] Artículo 5 *c) Dictará instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica., d) Dictará recomendaciones de aplicación de las disposiciones legales y reglamentarias en materia de seguridad de los datos y control de acceso a los ficheros.*

afectados, el artículo 37 de la LOPD y el Estatuto atribuyen a la Agencia la función de informar a las personas de los derechos que la Ley les reconoce en esta materia, pudiendo promover, a tal efecto, campañas de difusión, valiéndose de los medios de comunicación social, así como atender las peticiones y reclamaciones formuladas por las personas afectadas.

En el artículo 11 del Estatuto de la Agencia, se distinguen los órganos que conforman la estructura de la AEPD, tales como el Director, el Consejo Consultivo, el Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General, siendo los tres últimos, órganos jerárquicamente dependientes del Director de la Agencia. De lo mencionado, pueden distinguirse dos tipos de órganos, unos de carácter ejecutivo y otro cuya función es la de asesoramiento. El primer grupo está formado por el Director de la Agencia, el Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General. El Consejo Consultivo es el órgano asesor. Los órganos que conforman la estructura de la Agencia, así como las funciones que éstos desempeñan se analizan a continuación.

c) El Director:

Según lo establece el art. 36 de la LOPD[158], el Director dirige la Agencia y ostenta la representación de la misma, ejerce sus funciones con plena independencia y objetividad. El Director de la

[158] *Artículo 36. El Director*
1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.
2. Ejercerá sus funciones con plena independencia y objetividad, y no estará sujeto a instrucción alguna en el desempeño de aquéllas.
En todo caso, el Director deberá oír al Consejo Consultivo en aquéllas propuestas que éste le realice en el ejercicio de sus funciones.
3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1 a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.
4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

AEPD, con rango de Subsecretario, no estará sujeto a instrucción de autoridad alguna. Deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

En el Estatuto[159] de la Agencia se distingue entre las funciones de dirección y las funciones de gestión que corresponden al Director, de la siguiente manera:

Funciones de dirección:

Son aquellas en las que el Director dictará las resoluciones e instrucciones que se requieran en relación con las competencias que corresponden a la Agencia. Dentro de ellas, destacan las referentes a procedencia o improcedencia de las inscripciones en el Registro General de Protección de Datos, requerimientos a los

[159] *Sección 2. El Director de la Agencia de Protección de Datos*
Artículo 12. Funciones de dirección.
1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación.
2. Corresponde al Director de la Agencia de Protección de Datos dictar las resoluciones e instrucciones que requiera el ejercicio de las funciones de la Agencia y, en especial:
a) Resolver motivadamente sobre la procedencia o improcedencia de las inscripciones que deban practicarse en el Registro General de Protección de Datos.
b) Requerir a los responsables de ficheros de titularidad privada a que subsanen deficiencias de los códigos tipo.
c) Resolver motivadamente, previo informe del responsable del fichero, sobre la procedencia o improcedencia de la denegación, total o parcial, del acceso a los ficheros policiales o tributarios automatizados.
d) Autorizar transferencias temporales o definitivas de datos que hayan sido objeto de tratamiento automatizado o recogidos a tal efecto, con destino a países cuya legislación no ofrezca un nivel de protección equiparable al de la Ley Orgánica 5/1992 y el presente estatuto.
e) Convocar regularmente a los órganos competentes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación.
f) Recabar de las distintas Administraciones Públicas la información necesaria para el cumplimiento de sus funciones.
g) Solicitar de los órganos correspondientes de las Comunidades Autónomas, a que se refiere el artículo 40 de la Ley Orgánica 5/1992, la información necesaria para el cumplimiento de sus funciones, así como facilitar a aquéllos la información que le solicite n a idénticos efectos.
h) Adoptar las medidas cautelares y provisionales que requiera el ejercicio de la potestad sancionadora de la Agencia con relación a los responsables de los ficheros privados.
i) Iniciar, impulsar la instrucción y resolver los expedientes sancionadores referentes a los responsables de los ficheros privados.
j) Instar la incoación de expedientes disciplinarios en los casos de infracciones cometidas por órganos responsables de ficheros de las Administraciones Públicas.
k) Autorizar la entrada en los locales en los que se hallen los ficheros, con el fin de proceder a las inspecciones pertinentes, sin perjuicio de la aplicación de las reglas que garantizan la inviolabilidad del domicilio.

responsables de los ficheros de titularidad privada para que subsanen deficiencias de los códigos-tipo, procedencia o improcedencia de la denegación del acceso a algunos ficheros automatizados, autorización o denegación de transferencias internacionales de datos a países con un nivel de protección no adecuado, adopción de medidas cautelares y acuerdos de iniciación en relación con el ejercicio de la potestad sancionadora respecto a responsables de ficheros privados, solicitud de incoación de expedientes disciplinarios contra los responsables de ficheros públicos, y autorización de entrada en los locales en que se hallen los ficheros con el fin de proceder a las inspecciones que sean pertinentes.

Funciones de gestión:

Son aquellas en las que el Director actúa en relación con la ejecución de la actividad económico-financiera de la Agencia. A tal fin adjudica, formaliza y controla el seguimiento de los contratos de la Agencia, aprueba los gastos y ordena los pagos, ejerce el control económico-financiero de la Agencia, programa su gestión, elabora el anteproyecto de presupuesto, propone la relación de puestos de trabajo, aprueba la Memoria Anual de la Agencia y ordena la convocatoria de las reuniones del Consejo Consultivo. En relación con estas funciones el Director podrá delegar en el Secretario General todas ellas, salvo las que se refieren al control económico-financiero de la Agencia, a la aprobación de la Memoria Anual, y a la ordenación de las convocatorias del Consejo Consultivo. Por Resolución del Director de la Agencia, de 16 de febrero de 2004[160], se delegaron en el Secretario General diversas competencias[161].

[160] B.O.E. de 2 de marzo, RESOLUCIÓN de 16 de febrero de 2004, de la Agencia Española de Protección de Datos, por la que se delegan en el Secretario General de la Agencia determinadas competencias. *El art. 13,2 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, establece que el Director de la misma podrá delegar en el Secretario General el ejercicio de las funciones de gestión salvo las referidas al ejercicio del control económico-financiero, a la aprobación de la Memoria Anual y a la convocatoria de las reuniones del Consejo Consultivo. En consecuencia, a tenor de lo previsto en el artículo 13 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispongo: Primero.- Delegar en el Secretario General de la Agencia Española de Protección de Datos las siguientes competencias: a. Autorización, adjudicación y formalización de los contratos que realice la Agencia Española de Protección de Datos. b. Aprobación de las provisiones y cuentas*

d) El Consejo Consultivo:

Es el Órgano colegiado de asesoramiento del Director de la AEPD. A él le corresponde la función de emitir informe en relación con todas las cuestiones que le someta el Director, y podrá formular propuestas sobre temas relacionados con las materias de competencia de la AEPD. Su composición se encuentra establecida en el artículo 38 de la LOPD, que reza *"El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros: Un vocal por el Congreso de los Diputados, Un vocal por el Senado, un vocal de la Administración General del Estado propuesto por el Ministro de Justicia, un vocal de cada Comunidad Autónoma que haya creado una Agencia de Protección de Datos, un vocal de la Administración Local propuesto por la Federación Española de Municipios y Provincias, un vocal por la Real Academia de la Historia, un vocal por el Consejo de Universidades, un vocal de los usuarios y consumidores propuesto por el Consejo de Consumidores y Usuarios, un vocal del sector de ficheros privados propuesto por el Consejo Superior de Cámaras de Comercio, Industria y Navegación. Actúa como Presidente del Consejo Consultivo el Director de la AEPD y como Secretario, con voz y sin voto, el Secretario General de la Agencia. El Consejo Consultivo se reunirá cuando así lo decida el Director de la AEPD, que, en todo caso, lo convocará una vez cada seis meses. También se reunirá cuando así lo solicite la mayoría de sus miembros".*

En el año 2004 se incorporó al Consejo Consultivo, el Director de la Agencia Vasca de Protección de Datos, que fue nombrado en el mes de mayo, como consecuencia de la entrada en vigor de la Ley Vasca 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter

justificativas del sistema de anticipos de caja fija. c. Ordenación de pagos dentro de los límites presupuestarios. d. Autorización de comisiones de servicio. e. Programación de la gestión administrativa y financiera de la Agencia Española de Protección de Datos. f. Elaboración del proyecto de presupuesto anual. g. Proposición de modificación de la Relación de Puestos de Trabajo. Segundo.-Queda sin efecto la Resolución del Director de la Agencia Española de Protección de Datos de 24 de abril de 1998. Tercero.-La presente resolución entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado. Madrid, 16 de febrero de 2004.-El Director, José Luís Piñar Mañas.

[161] Memoria de la Agencia Española de Protección de Datos, año 2005, p. 33-34

Personal de Titularidad Pública y de creación de dicha Agencia autonómica[162].

e) El Registro General de Protección de Datos:

El Registro General de Protección de Datos es el órgano al que corresponde velar por la publicidad de la existencia de los ficheros de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de acceso, rectificación, oposición y cancelación regulados en los artículos 14 a 16 de la LOPD. El artículo 14 de la LOPD establece el derecho de consulta al Registro General de Protección de Datos y dispone que *"cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita"*.

El Estatuto de la AEPD[163], establece que corresponde al Registro General de Protección de Datos, instruir los expedientes de inscripción, expedir certificaciones de los asientos y publicar una relación anual de los ficheros notificados e inscritos. Así mismo, el artículo 39 de la Ley 15/1999, dispone que serán objeto de inscripción en el Registro, los ficheros de que sean titulares las Administraciones Públicas, los ficheros de titularidad privada, las autorizaciones de transferencias internacionales, los códigos tipo y los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

El contenido de la inscripción se encuentra regulado en el artículo 20 de la LOPD[164], para los ficheros de titularidad pública y

[162] Memoria de la Agencia Española de Protección de Datos, Año 2005, p. 36.
[163] Artículo 26 del Estatuto de la Agencia Española de Protección de Datos.
[164] *Artículo 20. Creación, modificación o supresión*
1. La creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.
2. Las disposiciones de creación o de modificación de ficheros deberán indicar:
a) La finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

en el artículo 26[165] para los ficheros de titularidad privada. Además, por vía reglamentaria se ha regulado el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Estos aspectos se encuentran regulados también por el Real Decreto 1332/1994, de 20 de junio, que desarrolla determinados aspectos de la LORTAD, y que continúa vigente a tenor de lo dispuesto en la disposición transitoria tercera de la LOPD. Por otro lado, también se encuentra vigente la Resolución de 12 de julio de 2006[166], de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro

c) El procedimiento de recogida de los datos de carácter personal.
d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
f) Los órganos de las Administraciones responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.
3. En las disposiciones que se dicten para la supresión de los ficheros se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

[165] *Artículo 26. Notificación e inscripción registral*
1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.
2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.
4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

[166] Este documento se vio modificado por la Resolución de 8 de septiembre de 2006, de la Agencia Española de Protección de Datos, por la que se corrigen errores en las Resoluciones de 12 de julio de 2006, por las que se crea el Registro Telemático y se aprueban los formularios electrónicos para inscribir los ficheros en el Registro General de Protección de Datos.

General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático.

Así mismo, se ha dictado en este ámbito, la Resolución de 1 de septiembre de 2006, de la AEPD, por la que se determina la información que contiene el Catálogo de ficheros inscritos en el Registro General de Protección de Datos.

Cabe destacar la importancia de los principios de la inscripción de ficheros, entre ellos la obligación del responsable del fichero de efectuar una notificación para su inscripción en el Registro, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos. Por otro lado el hecho de que la inscripción de un fichero de datos es declarativa, es decir, no prejuzga que se hayan cumplido el resto de las obligaciones derivadas de la LOPD. Así también, el principio de que la notificación de ficheros implica el compromiso por parte del responsable de que el tratamiento de datos personales declarados para su inscripción cumple con todas las exigencias legales.

Finalmente, es menester destacar que la notificación de los ficheros al Registro supone, una obligación de los responsables del tratamiento, sin coste económico alguno para ellos, y facilita que las personas afectadas puedan conocer quienes son los titulares de los ficheros ante los que deben ejercitar directamente los derechos de acceso, rectificación, cancelación y oposición[167].

f) La Secretaría General:

Los artículos 30 y 31 del Estatuto de la Agencia crean la Secretaría General, que conforme a esta norma, posee básicamente funciones de apoyo, ejecución y documentación las cuales se resumen en las siguientes:

Funciones de apoyo y ejecución: Elaborar los informes y propuestas que les solicite el Director, notificar las resoluciones del Director, ejercer la secretaría del Consejo Consultivo, gestionar los

[167] A. CANALES GIL, *La Agencia Española de Protección de Dato: Estructura y Funcionamiento*, II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. 2ª Edición Protección de datos de carácter personal en Iberoamérica. Tirant lo Blanch, Valencia, 2006, p. 299

medios personales y materiales, así como atender la gestión económico-administrativa de la AEPD, llevar el inventario, y cuantos asuntos no estén atribuidos a otros órganos de la misma.

Otras funciones: Formar y actualizar el fondo de documentación en materia de protección de datos, editar los repertorios oficiales de ficheros inscritos en el Registro General de Protección de Datos, las memorias anuales y cualesquiera otras publicaciones de la AEPD, organizar conferencias, seminarios y cualesquiera otras actividades de cooperación internacional e interregional sobre protección de datos y facilitar la información necesaria para llevar a cabo campañas de difusión a través de los medios de comunicación. Cabe destacar que dentro de la Secretaría General se encuentra el Área de Atención al Ciudadano, la cual tiene la función primordial de informar a los ciudadanos, de la forma más sencilla posible, sobre aquellas cuestiones que les preocupan directamente, por lo tanto, esta área de la Agencia constituye en la mayoría de las ocasiones, la primera aproximación que tiene a su disposición el ciudadano para poder informarse y plantear aquellas consultas que considere necesarias en orden a la aplicación de la LOPD a su caso concreto, a fin de lograr una mejor defensa de sus derechos[168].

g) La Inspección de Datos:

Los artículos 27, 28 y 29 del Estatuto de la Agencia, crean la Inspección de Datos como órgano adscrito a la Agencia Española de Protección de Datos al que competen las funciones inspectoras previstas en el artículo 40 de la LOPD[169]. Específicamente dentro del ámbito de la Agencia, la inspección es desempeñada por la Subdirección General de Inspección de Datos, órgano bajo la dirección y superior autoridad del Director, al cual le corresponde desempeñar dos de las más importantes funciones para el efectivo cumplimiento de la LOPD, por un lado la función inspectora o investigadora y por otro la función instructora de los expedientes sancionadores y procedimientos de tutela de derechos las cuales se detallan a continuación.

[168] Memoria de la Agencia Española de Protección de Datos, Año 2005.
[169] G. FREIXAS GUTIÉRREZ, *La protección de datos de carácter personal en el derecho español*, Bosh, Barcelona. 2001 p.310.

Función inspectora:

La Inspección de Datos no se encuentra contemplada por la Ley 15/1999 desde la vertiente orgánica, sino sólo desde la funcional, siendo el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la AEPD, el que prevé que las funciones inherentes al ejercicio de la potestad de inspección que el art. 40 de la LOPD atribuye a la Agencia, se ejerzan por un órgano específico y separado de los demás al frente del cual se sitúa a un funcionario con categoría de Subdirector General.

Es posible observar que el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la AEPD no añade nuevas precisiones sobre el estatuto personal de quienes se encuadran en este órgano a las ya contenidas en la LOPD, la cual dispone que los funcionarios que ejerzan funciones inspectoras tendrán la consideración de autoridad pública en el desempeño de sus cometidos[170], de donde resulta que la inspección deberá ser desempeñada por funcionarios de carrera. El carácter de "autoridad pública" que el artículo 40.2 LOPD atribuye a los Inspectores de Datos significa que las personas responsables de los ficheros y/o tratamientos que ofrezcan resistencia o cometan atentado contra dichos funcionarios/inspectores, podrían incurrir en su caso en responsabilidad penal, exigible conforme a la legislación penal, y en todo caso incurrirían en la responsabilidad administrativa prevista en el art. 44.3.j) de la LOPD, calificada como obstrucción al ejercicio de la función inspectora[171].

El Estatuto[172] desarrolla el contenido de la potestad de inspección atribuida a la Agencia en el ya citado art. 40 de la LOPD, precisando la facultad de la Inspección de Datos para efectuar inspecciones de oficio, aunque pudieran también tener su origen en una denuncia de las personas afectadas, y detallando el alcance concreto de su capacidad para requerir y obtener información, así como examinar in situ los ficheros y sistemas informáticos en los que se traten datos de carácter personal. En conjunto, se trata de

[170] Artículo 40, LOPD.

[171] Por lo tanto, la persona que obstruyera el ejercicio de la función inspectora incurriría en infracción grave, según lo establecido en la LOPD y sancionada con multa de 60.101,21 a 300.506,05 euros por el artículo 45 de la mencionada Ley.

[172] Artículo 28.1

una serie de facultades cuya finalidad es la de obtener información y, en su caso, pruebas sobre posibles incumplimientos de la LOPD, que permitan posteriormente al órgano decisorio incoar procedimientos sancionadores y adoptar, en su caso, las medidas pertinentes dirigidas a la cesación de actividades ilícitas en los términos previstos en los artículos 37.f)[173] y 49[174] de dicha Ley.

Así mismo, en el marco de la función inspectora, se impone a los funcionarios que la ejercen el deber de guardar secreto sobre las informaciones que conozcan en el ejercicio de tal función, incluso después de haber cesado en la misma[175]; deber cuyo incumplimiento generaría la oportuna responsabilidad disciplinaria mientras se conserve la relación de servicio con la AEPD, y que se reputaría infracción administrativa grave, una vez extinguida dicha relación, al amparo del art. 44.3 g)[176] de la LOPD.

Función instructora:

Corresponde también a la Subdirección General de Inspección de Datos la función instructora en los expedientes sancionadores, es decir, el ejercicio de los actos de instrucción

---

[173] *"Funciones de la Agencia Española de Protección de Datos: Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones".*

[174] *"Potestad de inmovilización de ficheros: En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas".*

[175] Artículo 40.2 de la LOPD y artículo 27.2 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

[176]*"Son infracciones graves g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo".*

relativos a los expedientes sancionadores, según lo establece el artículo 29 del Estatuto de la Agencia.

El ejercicio de esta función instructora correspondiente a la Subdirección General de Inspección de Datos, no es más que la consecuencia obligada de la existencia de la potestad sancionadora atribuida en exclusiva al Director de la Agencia[177] y la necesaria garantía del procedimiento sancionador, cuyo ejercicio exige la separación entre la fase instructora y la sancionadora, encomendándolas a órganos distintos[178].

El procedimiento sancionador, de conformidad con lo previsto en el art. 48.1 de la LOPD, está regulado en el Real Decreto 1332/1994[179], de 20 de junio, por el que se desarrollan determinados aspectos de la LORTAD, que detalla el cauce a seguir para la determinación de las infracciones y la imposición de sanciones, estructurándose como cualquier otro procedimiento sancionador en las tres clásicas fases de Iniciación, Instrucción y Resolución, correspondiendo al funcionario instructor el desarrollo completo de la fase de Instrucción u Ordenación del procedimiento y la propuesta razonada al Director de la Agencia de las otras dos, es decir, del acuerdo de inicio del procedimiento sancionador y de la Resolución del mismo.

Por otra parte, la función instructora se concreta en la incoación de tres clases de procedimientos, en primer lugar el procedimiento sancionador incoado contra los responsables de ficheros de titularidad privada por infracción de los principios y reglas contenidos en la LOPD; en segundo lugar, el procedimiento por infracciones de las Administraciones Públicas[180], cuando es una

[177] Artículo. 37 g) LOPD: *"g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley"*.

[178] Artículo 134 Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común: "*Garantía de procedimiento. 1. El ejercicio de la potestad sancionadora requerirá procedimiento legal o reglamentariamente establecido. 2. Los procedimientos que regulen el ejercicio de la potestad sancionadora deberán establecer la debida separación entre la fase instructora y la sancionadora, encomendándolas a órganos distintos. 3. En ningún caso se podrá imponer una sanción sin que se haya tramitado el necesario procedimiento"*.

[179] El cual se encuentra aún en vigor en tanto no se dicte otra disposición reglamentaria en desarrollo de la LOPD y en tanto no contravenga lo dispuesto por esta norma.

[180] Artículo 46 LOPD: *"Infracciones de las Administraciones Públicas 1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las*

Administración de esta clase la que vulnera los preceptos de la Ley; y en tercer lugar el procedimiento de tutela de derechos previsto en el art. 18 de la Ley, que se actúa cuando son vulnerados los derechos de oposición, acceso, rectificación o cancelación de los afectados establecidos en los artículos 15 a 17 de la mencionada norma.

El procedimiento de tutela de derechos supone la existencia de un posible incumplimiento de la Ley que no sea constitutivo de infracción, lo que justifica referirse a esta potestad arbitral de tutela al margen de la potestad sancionadora de la Agencia. La nueva LOPD ha venido a reproducir el mismo esquema que regía bajo la vigencia de la derogada LORTAD, si bien ha introducido dos novedades en el procedimiento de tutela de derechos al ampliar el plazo máximo para dictar resolución a seis meses establecido en el artículo 18.3 de la LOPD, siguiendo la pauta general que para los procedimientos administrativos establece el art. 42.2 la Ley 30/1992, de 26 de noviembre, y dar entrada en la regulación de estos procedimientos a un nuevo derecho que se desconocía en la anterior legislación: el derecho de oposición, dispuesto en el artículo 6.4 de la LOPD.

Finalmente, la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, ha introducido algunas modificaciones en el régimen de la AEPD, el art. 82 ha introducido modificaciones en el art. 37 de la LOPD, que a partir del 1 de enero de 2004, las resoluciones de la AEPD debían hacerse públicas, una vez hubieran sido notificadas a los interesados. La Agencia, a través de la Instrucción 1/2004, de 22 de diciembre, ha regulado la forma y los plazos en que ha de realizarse esta publicación.

Administraciones Públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera. 2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores. 4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores".

h) Actividades y relaciones internacionales:

En lo que respecta a las relaciones internacionales, el referido art. 37 l) de la LOPD[181] y el Estatuto de la Agencia[182]atribuyen a la ésta las funciones de cooperación internacional en materia de protección de datos personales. En este ámbito, se dispone que la Agencia prestará asistencia a las autoridades designadas por los Estados parte en el Convenio del Consejo de Europa de 28 de enero de 1981, sobre protección de las personas en relación con el tratamiento automatizado de los datos de carácter personal, a los efectos previstos en el artículo 13 del Convenio y se designa a la Agencia, como representante español a los efectos previstos en el art. 29 de la Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, correspondiendo al Director de la Agencia, la designación de un representante para el Grupo de Protección de las Personas en lo que respecta al tratamiento de datos personales, previsto en la disposición citada.

Así mismo, dispone el Estatuto que la Agencia ejercerá el control de los datos de carácter personal introducidos en la parte nacional española, de la base de datos del Sistema de Información de Schengen (SIS), correspondiendo al Director, la designación de dos representantes para la autoridad de control común de protección de datos del citado SIS.

La Red Iberoamericana de Protección de Datos:

Se debe reconocer la importante iniciativa por parte de la AEPD, de impulsar las vías de colaboración internacional con Iberoamérica, entendiendo que el nacimiento de esa área geográfica y cultural al derecho a la protección de datos de carácter personal debería producirse desde la perspectiva de un intercambio global de experiencias puestas en común desde los diferentes ámbitos de decisión.

[181] *l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.*

[182] Modificado en este punto por el Real Decreto 156/1996, de 2 de febrero.

La creación de la Red Iberoamericana de Protección de Datos, se produjo en junio de 2003 con ocasión de la celebración del II Encuentro Iberoamericano de Protección de Datos, el cual tuvo lugar en La Antigua (Guatemala).Este Encuentro contó con la participación de 15 de los entonces 21 Estados[183] que conformaban la Comunidad Iberoamericana.

Los participantes, en la Declaración firmada al finalizar este Encuentro, resaltaron la necesidad de dotar de una estructura permanente a este foro con el objeto de reforzar la mutua y continua colaboración entre todos y de abrirla a la incorporación de representantes de todos los países Iberoamericanos. En esta Declaración de La Antigua, los participantes reiteraron la consideración de la protección de datos personales como un auténtico derecho fundamental[184] y declararon que el tratamiento de los datos personales puede impulsar el desarrollo de los Países Iberoamericanos, en el marco de la sociedad de la información y para la consecución de sus legítimos fines por parte de los sectores público y privado, reconociendo los grandes beneficios que las nuevas tecnologías de la Información y las Comunicaciones puede suponer para el desarrollo social y económico de los países[185].

En la Declaración los firmantes reconocen que todavía en Iberoamérica se producen situaciones que impiden o dificultan el ejercicio efectivo del derecho[186], constatan la necesidad de adoptar medidas que garanticen un elevado nivel de protección de datos y tener marcos normativos que garanticen una adecuada protección en todos los países iberoamericanos que deberían tomar en consideración los principios esenciales de protección de datos reconocidos en los Instrumentos Internacionales[187]. En esta Declaración, en la que se plasma la creación de la Red, se establece una Presidencia y una Secretaría Permanente, que radican en la AEPD.

[183] Actualmente la Comunidad Iberoamericana está integrada por 22 Estados, tras la reciente incorporación de Andorra.
[184] Artículo 2º de la Declaración de la Antigua.
[185] Artículo 3º de la Declaración de la Antigua.
[186] Artículo 4º de la Declaración de la Antigua.
[187] Artículo 5º de la Declaración de la Antigua.

Cabe agregar que la Red fue expresamente reconocida al más alto nivel político, ya que en la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, en Santa Cruz de la Sierra (Bolivia), en la Declaración Final, en su apartado 45, se recogió expresamente lo siguiente: *"Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad."*[188]

B. Las Agencias Autonómicas de Protección de Datos:

La Ley 15/1999 Orgánica de Protección de Datos, en su artículo 41.1[189] contempla expresamente la posibilidad de que en cada Comunidad Autónoma se cree un órgano encargado de velar por los derechos y libertades de los ciudadanos en esta materia. En función de lo dispuesto en la LOPD, han creado su propia Agencia Autonómica de Protección de Datos Madrid, Cataluña y el País Vasco, estando en fase de aprobación la normativa de la Comunidad Valenciana que crea la Agencia de Protección de Datos y en fase de elaboración la correspondiente norma de Castilla-La Mancha[190]. Las Agencias autonómicas, son entes de derecho público "independientes", al igual que la estatal; no responden a órdenes, instrucciones ni a directrices administrativas. Su estructura orgánica es similar a la de la Agencia Española de Protección de Datos y se encuentran compuestas por un Consejo Consultivo, un Director y un Registro de Ficheros de Datos Personales, dependiente del Director.

[188] Memoria de la Agencia Española de Protección de Datos, Año 2005, p. 113

[189] *"Órganos correspondientes de las Comunidades Autónomas 1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido"*.

[190] M. ARENAS, *El derecho fundamental a la protección de datos personales en Europa*, Agencia Española de Protección de Datos, Tirant lo Blanch, Valencia, 2006. p. 589-590.

En lo que respecta al Consejo Consultivo que posee cada una de la Agencias Autonómicas, cabe resaltar la mayor relevancia que estos ostentan con relación al rol que desempeña el Consejo de la AEPD. Así, por ejemplo es digno destacar el hecho de que en Cataluña el Presidente del Consejo no es el Director de la Agencia[191], como ocurre en la estatal y en la Agencia de Protección de Datos de la Comunidad de Madrid, sino que es nombrado por el Presidente de la Generalidad de Cataluña y asiste al Consejo con voz, pero sin voto. Por su parte, el Consejo Consultivo de la Agencia Vasca de Protección de Datos tiene potestad conferida por el artículo 16.2 de la Ley 2/2004 del Parlamento Vasco, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, para aprobar sus propias normas de organización y funcionamiento, en las que se preverán las figuras de presidente y secretario, así como el sistema para su elección o designación. El Estudio y aprobación del Reglamento de Funcionamiento Interno del Consejo Consultivo tuvo lugar el 1 de abril del año 2006, siendo electo presidente del Consejo Consultivo uno de sus miembros, diferenciándose también de la Agencia Estatal en donde el cargo Presidente del Consejo es desempeñado por el Director de la Agencia .

En relación con el Director, a diferencia de la forma de elección del Director de la AEPD, en la Comunidad de Madrid se exige que el Director sea "previamente designado" por el Consejo Consultivo, lo que refuerza su carácter independiente, y se exige también que el mismo tenga conocimientos técnicos en la materia; en Cataluña se dice únicamente que se le nombrará "a propuesta" del Consejo Consultivo; y en el País Vasco, al igual que en la AEPD, el Consejo Consultivo no interviene a la hora del nombramiento del Director. Por último, señalar que las Agencias Autonómicas de Protección de Datos, al igual que la AEPD, disponen de una serie de recursos para cumplir con sus fines y funciones, que se establecen con cargo a los Presupuestos de la Comunidad Autónoma, y

[191] Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos. Artículo 14. 3. *"El presidente o presidenta del Consejo es nombrado por el presidente o presidenta de la Generalidad, a propuesta del titular del departamento con el cual se relaciona la Agencia, de entre una terna presentada por el Consejo Asesor entre sus miembros. Actúa de secretario un funcionario de la Agencia Catalana de Protección de Datos"*.

cuentan además con subvenciones y aportaciones que se concedan a su favor.

En cuanto a las competencias[192], hay que señalar que las Agencias Autonómicas de Protección de Datos tienen las mismas competencias que la estatal, a excepción, como dice el artículo 41 LOPD, de las competencias relacionadas con las transferencias internacionales de datos, la publicidad de los tratamientos y la redacción de una Memoria Anual. Aquí hay que señalar que, en realidad, no se trata de competencias reservadas a la Administración del Estado, sino desarrolladas, en principio, por la AEPD, sin perjuicio de que también puedan ser desarrolladas por las Agencias Autonómicas, como ocurre actualmente con la redacción de las Memorias Anuales.

La diferencia fundamental entre la AEPD y las autonómicas reside en el diferente ámbito de actuación de una y otras. El ámbito de actuación de estos organismos autonómicos se encuentra restringido al territorio de la propia Comunidad Autónoma y a los ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local situada en el territorio de la Comunidad. La LORTAD, y actualmente la LOPD[193], excluyen, en todo caso, la competencia de las Agencias autonómicas sobre los ficheros de titularidad privada, y es aquí, donde surgió el conflicto sobre la distribución de competencias entre la Agencia estatal y las autonómicas.

Por último, es menester hacer referencia a la relación existente entre la AEPD y las Agencias Autonómicas. Parece claro que la relación no puede ser de jerarquía, sino de coordinación, ya que cada una desarrolla sus competencias en ámbitos diferentes, si bien han de actuar coordinadamente para no provocar situaciones de agravio o discriminación por razón de la titularidad del fichero. Si la garantía del derecho a la protección de datos personales es competencia del Estado, éste deberá actuar bajo el principio de coordinación, desarrollando los instrumentos de dirección y

[192] En el artículo 41 LOPD, además de reconocerse la posibilidad de creación de Autoridades de control a nivel autonómico, se definen las competencias de estas autoridades y su ámbito de actuación.
[193] Artículo 41.1 de la LOPD

ordenación necesarios para que la protección de datos funcione "coordinadamente" en todo el territorio nacional[194].

C. El Defensor del Pueblo:

Esta institución encargada de garantizar la protección de los derechos fundamentales frente a la actuación de los poderes públicos, especialmente la Administración, también puede conocer de aquellos casos en que los sujetos consideren que se ha lesionado su derecho a la protección de datos personales. No obstante, en la práctica, los ciudadanos antes de acudir a un órgano como el Defensor del Pueblo para garantizar el derecho a la protección de datos personales, acuden a la Agencia Española de Protección de Datos o a la Agencia autonómica competente, si fuera el caso.

El ciudadano que considere que algún órgano administrativo ha lesionado su derecho a la intimidad o su derecho a la protección de datos personales, puede acudir a la vía administrativa y una vez agotada ésta, a la contencioso-administrativa, sin perjuicio del recurso al Defensor del Pueblo[195].

En España el Defensor del Pueblo recibe las quejas de los ciudadanos por la actuación administrativa, pudiendo recibir también las relativas a la protección de datos personales, y la LOPD prevé, para el caso de que la infracción cometida en un tratamiento de datos sea consecuencia de la actuación de una Administración Pública, que el Director de la AEPD, comunique al Defensor del Pueblo las actuaciones y resoluciones que el mismo realice[196].

[194] M. ARENAS, *El derecho fundamental a la protección de datos personales en Europa*, op. cit. p. 592

[195] Ley Orgánica 3/1981, de 6 de abril, del Defensor del Pueblo, Artículo 9. 1. "*El Defensor del Pueblo podrá iniciar y proseguir de oficio o a petición de parte, cualquier investigación conducente al esclarecimiento de los actos y resoluciones de la Administración pública y sus agentes, en relación con los ciudadanos, a la luz de lo dispuesto en el artículo 103.1 de la Constitución, y el respeto debido a los derechos proclamados en su Título primero dos. Las atribuciones del Defensor del Pueblo se extienden a la actividad de los ministros, autoridades administrativas, funcionarios y cualquier persona que actúe al servicio de las administraciones públicas*".

[196] Artículo 46.4 de la LOPD.

2. Garantías Jurisdiccionales:

En España se ha establecido un sistema de garantías de los derechos fundamentales, garantías que incluyen mecanismos tanto preventivos como reparadores. El derecho a la protección de datos personales, en tanto que derecho fundamental, ya sea autónomo, ya sea como parte integrante del ámbito protegido por otro derecho fundamental, disfruta de la protección que en cada ordenamiento jurídico nacional se establezca para los derechos fundamentales.

Ante una violación del derecho a la protección de datos personales el titular de los mismos puede acudir a la vía judicial ordinaria, dependiendo del tipo de vulneración cometida frente al derecho a la protección de datos personales, además del recurso contencioso-administrativo que pueda interponerse frente a las decisiones de la Agencia Española de Protección de Datos, cabe acudir a la vía civil o penal.

En lo que respecta al procedimiento contencioso-administrativo, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la AEPD en el plazo de un mes a contar desde el día siguiente a la notificación de la resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25[197]y en el apartado 5 de la disposición adicional cuarta[198] de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal y las sentencias emanadas de la

[197] Artículo 25. 1. *"El recurso contencioso-administrativo es admisible en relación con las disposiciones de carácter general y con los actos expresos y presuntos de la Administración pública que pongan fin a la vía administrativa, ya sean definitivos o de trámite, si estos últimos deciden directa o indirectamente el fondo del asunto, determinan la imposibilidad de continuar el procedimiento, producen indefensión o perjuicio irreparable a derechos o intereses legítimos.2. También es admisible el recurso contra la inactividad de la Administración y contra sus actuaciones materiales que constituyan vía de hecho, en los términos establecidos en esta Ley"*.

[198] *5. "Los actos administrativos dictados por la Agencia de Protección de Datos, Comisión del Sistema Eléctrico Nacional, Comisión del Mercado de las Telecomunicaciones, Consejo Económico y Social, Instituto* Cervantes, *Consejo de Seguridad Nuclear y Consejo de Universidades, directamente, en única instancia, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional"*

Audiencia Nacional podrán ser recurridas a su vez ante el Tribunal Supremo.

En el caso de que el afectado desee reclamar su derecho previsto en el artículo 19 de la LOPD, que establece que los interesados que como consecuencia del incumplimiento de lo dispuesto en la Ley sufran daño o lesión en sus bienes o derechos, tendrán derecho a ser indemnizados, la vía a la que deberá acudir será la jurisdicción ordinaria a través de lo civil, y será ésta la que determinará cualquier responsabilidad y el derecho a una indemnización[199]. En lo que respecta al caso de los ficheros de titularidad pública, el afectado deberá recurrir según lo establecido en el Real Decreto 429/1993, de 26 de marzo, por el que se aprueba el Reglamento de los procedimientos de las Administraciones Públicas en materia de de responsabilidad patrimonial[200].

Por otro lado, cabe recordar que en España, el legislador dio cumplimiento al mandato de limitar el uso de la informática establecido en el artículo 18.4 de la Constitución Española aprobando, en primer lugar, la Ley Orgánica 1/1982, de 5 de mayo de Protección Civil del Derecho al Honor, a la Intimidad y a la Propia Imagen, que regula la defensa de la intimidad frente a las agresiones producidas por medios tecnológicos y permite al titular acudir a la vía civil en defensa de su intimidad; y, en segundo lugar, tipificando en la Ley Orgánica 10/1995, de 23 de noviembre del Código Penal, los delitos informáticos que permiten al titular del derecho a la intimidad o a la protección de datos personales acudir a la vía penal[201].

---

[199] El derecho a la indemnización no puede ser reclamado ante la Agencia Española de Protección de Datos, ya que ésta no se encuentra facultada para ello. Por otro lado, si es posible efectuar una denuncia ante este organismo, a fin de que inicie el proceso sancionador correspondiente, para lo cual la Agencia si tiene potestad reconocida por la LOPD en su artículo 37 g).

[200] G. FREIXAS GUTIÉRREZ, *La protección de datos de carácter personal en el derecho español*, op. cit. p.199

[201] El artículo 197.2 supone una novedad y dispone : "*Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien sin estar autorizados, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero*".

Es importante agregar que los ciudadanos tienen la facultad de acudir, a fin de defender su derecho a la protección de datos personales, por la vía del recurso de amparo, el cual puede ser interpuesto ante el Tribunal Constitucional una vez agotada la vía judicial previa. En este sentido este Tribunal ha afirmado que *"la Norma Fundamental otorga una protección especial a los denominados derechos fundamentales y libertades públicas cuyo desarrollo está reservado a la Ley Orgánica y cuya tutela específica se realiza ante los Tribunales ordinarios, junto con la relativa al principio de igualdad del artículo 14 y a la objeción de conciencia del artículo 30 por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante este Tribunal"*[202]. Así mismo, y como se ha analizado previamente en el capítulo primero del presente trabajo, a partir de las Sentencias 290/2000 y 292/2000, no cabe duda de que se puede invocar directamente la vulneración de este derecho ante el Tribunal Constitucional, pues en ellas el Tribunal ha reconocido expresamente el carácter de derecho fundamental del derecho a la protección de datos personales.

II- Ámbito Europeo:

1. Consejo de Europa

El Consejo de Europa nació vinculado a la protección y garantía de los derechos humanos y ha sido el organismo internacional pionero que ha desarrollado con una mayor eficacia mecanismos de protección para los mismos, entre los que destaca el Tribunal Europeo de Derechos Humanos.

A. Tribunal Europeo de Derechos Humanos

Como apunta Lucas Murillo de la Cueva[203], el Tribunal Europeo de Derechos Humanos[204] ha sido sensible al movimiento

[202] Sentencia del Tribunal Constitucional Nº 18/1981, Fundamento Jurídico Nº 4

[203] P. LUCAS MURILLO DE LA CUEVA, *La protección de datos en la Administración de Justicia*, Derecho a la intimidad y las nuevas tecnologías, Cuadernos de Derecho Judicial IX, Consejo General del Poder Judicial, Madrid 2004 p.232.

[204] El TEDH se encarga de examinar, como hemos dicho, los asuntos que le sometan tanto los Estados como los particulares relativos a violaciones de los derechos y libertades protegidos por el CEDH y sus Protocolos Adicionales.

encaminado al reconocimiento del derecho a la autodeterminación informativa. A través de la interpretación del Convenio Europeo de Derechos Humanos, ha establecido que el derecho a la vida privada y familiar que se reconoce en su artículo 8 comprende el derecho a la protección de datos de carácter personal. Ciertamente, la fórmula utilizada por el Convenio Europeo, el derecho a la vida privada y familiar, sin duda, más amplia que el concepto de intimidad, ha facilitado el paso por el Tribunal de Estrasburgo, entre otras, en las Sentencias de 26 de marzo de 1987, caso Leander contra Suecia, Sentencia de 25 de marzo de 1998, caso Knopp contra Suiza, Sentencia 2000/87 caso Amann contra Suiza, Sentencia 2000/130, de 4 de mayo, caso Rotaru contra Rumania, esta última representa un cambio relevante en la medida en que atribuye una consistencia autónoma a la protección de datos frente al tronco constituido por la vida privada y familiar.

Por lo que respecta a la labor del TEDH respecto del derecho a la protección de datos personales garantizado por el artículo 8 del CEDH podemos decir que ha sido abundante. Así por ejemplo podemos recordar algunos de los primeros casos de protección de datos personales, los casos *Klass* y *Malone*, relativos a sistemas de escuchas o vigilancia. En estos casos el TEDH consideró que, aunque las medidas de vigilancia no iban dirigidas directamente contra los demandantes, debido a que la legislación vigente permitía el control del correo electrónico, del correo tradicional y de las telecomunicaciones, cualquier ciudadano del Estado en cuestión podría considerarse "víctima" y por lo tanto podía interponer una demanda (en este caso ante la Comisión porque todavía los particulares no podían acudir directamente ante el TEDH). Ya presentando la demanda ante el TEDH podemos recordar el caso *P.G. y J.H vs. Reino Unido*, en el que el TEDH consideró la grabación de las voces de los demandantes para un posterior análisis como un procesamiento de sus datos personales y por tanto, como una injerencia en su derecho[205].

Es necesario aclarar que las Sentencias del TEDH tienen un carácter declarativo y no ejecutivo, y es aquí donde se plantea el problema, en el amplio margen de discrecionalidad que en la

[205] M. ARENAS R., *El derecho fundamental a la protección de datos personales en Europa*, op. cit. p. 178

ejecución de las Sentencias se deja al Estado. Las Sentencias no podrán declarar nunca nula una norma de Derecho interno ni anular un acto administrativo que se estime contrario al CEDH, ya que el TEDH lo que hace es determinar la responsabilidad internacional del Estado y no la de la autoridad nacional a la que le es imputable la violación del CEDH, lo cual corresponde al Estado. Así, en el *caso Marckx,* el TEDH dejó claro que la *"sentencia del Tribunal es esencialmente declarativa y deja al Estado la decisión de los medios a utilizar en su ordenamiento jurídico interno".*

B. Las garantías Específicas en el marco del Consejo de Europa:

El derecho a la protección de datos personales se beneficia, en el marco del Consejo de Europa[206], no sólo de las garantías genéricas comunes a todos los derechos fundamentales, sino también de un conjunto de garantías específicas que se analizan a continuación.

a) El Comité de Expertos en Protección de Datos:

El Consejo de Europa crea en 1976 un Grupo de Expertos en Protección de Datos Personales[207]. Este Comité se compone de expertos de cada uno de los Estados miembros y desarrolla su labor a través de Recomendaciones sectoriales y a través de la cooperación con otras organizaciones en las que se tratan temas relativos a datos personales y con otros Comités del Consejo de Europa, como, por ejemplo, con el Grupo de Especialistas en Identificación y Terrorismo. De entre los documentos elaborados por este Comité podemos mencionar, por ejemplo, las Directrices para la protección de los datos personales en tarjetas personales.

[206] El Consejo de Europa comenzó a mostrar su preocupación por la garantía de este derecho a principios de los años setenta y creó entonces en 1976 un Grupo de Expertos en Protección de Datos que analizara la situación en ese momento, pero ha sido posteriormente, a través del Convenio 108 sobre Protección de Datos Personales, cuando se desarrollarían mejores garantías en la exigencia de Autoridades Independientes de Control de los tratamientos de datos personales.

[207] Denominado: Project Group on Data Protection, CJ-PD.

b) El Comité Consultivo:

El Convenio 108 establece un Comité Consultivo[208] específico al que se denomina T-PD. Cada Estado parte del Convenio 108 tiene un representante en el Comité Consultivo, que, en la práctica, suele ser un miembro de la Autoridad de Control nacional. El Comité tiene las funciones de: presentar propuestas con el fin de facilitar o de mejorar la aplicación del Convenio 108, presentar propuestas de enmienda al mismo y formular su opinión acerca de ellas, y expresar, a petición de una Parte, su opinión acerca de cualquier cuestión relativa a la aplicación del presente Convenio. Este Comité desarrolla una importante función a través de las propuestas que realiza para mejorar la aplicación del Convenio 108. Así mismo, es importante agregar que ha tomado la iniciativa en el estudio de la transferencia de datos personales y de otras materias importantes[209].

2. Unión Europea:

En el ámbito de la Unión Europea el derecho a la protección de los datos personales disfruta de las garantías genéricas previstas para todos los derechos, como ser el recurso ante el Tribunal de Justicia de las Comunidades Europeas y las reclamaciones ante el Defensor del Pueblo Europeo. Así también se encuentran previstas en el marco comunitario ciertas garantías específicas establecidas concretamente para asegurar el respeto a este derecho.

A. Garantías genéricas:

a) Tribunal de Justicia de las Comunidades Europeas:

Como bien lo expone ARENAS RAMIRO[210], el TJCE es la instancia suprema cuya función es garantizar el respeto del Derecho comunitario en la interpretación y aplicación de los

[208] Este Comité se reúne, al menos, una vez cada dos años y, en todo caso, cada vez que un tercio de los representantes de las Partes solicite su convocatoria. Después de cada una de dichas reuniones, el Comité Consultivo someterá al Comité de Ministros del Consejo de Europa una memoria acerca de sus trabajos y el funcionamiento del Convenio.

[209] Entre sus numerosos trabajos, destaca el Informe de situación relativo a la aplicación de los principios del Convenio 108 sobre la recogida y proceso de datos biométricos.

[210] M. ARENAS R., *El derecho fundamental a la protección de datos personales en Europa*, op. cit. p. 340

Tratados[211]. Por consiguiente, si un Estado o un ciudadano consideran que la Ley nacional de protección de datos personales vulnera lo establecido en la normativa comunitaria, puede acudir al TJCE y plantear recurso para que éste Órgano se pronuncie sobre dicha cuestión. Con la inclusión de la Carta de Derechos Fundamentales de la Unión Europea en el Tratado que establece la Constitución Europea, cuando la misma entre en vigor, se podrá invocar directamente ante el TJCE la violación del derecho fundamental, tal y como reconoce dicho Tratado. En estos casos se prevé también la posibilidad de utilizar una de las garantías específicas a nivel comunitario, un "amparo" ante el Supervisor Europeo. La necesidad de hacer frente al aumento de asuntos que le llegaban y mejorar la protección de los ciudadanos europeos, provocó la creación del Tribunal de Primera Instancia, encargado de conocer en primera instancia determinadas categorías de recursos[212].

Si bien es necesario reconocer que el TJCE no tiene competencia sobre los derechos fundamentales, materia que escapa del ámbito comunitario[213], sin embargo, en la práctica el TJCE ha desarrollado una importante labor en este ámbito. Al tener que determinar los límites de la aplicación del Derecho comunitario cuando éste colisiona con derechos fundamentales de los ciudadanos comunitarios, en realidad lleva a cabo una función "delimitadora" de los derechos.

[211] Es importante recordar aquí que, como hemos dicho, la actividad que desarrollen las instituciones y organismos de la Unión queda sometida a su competencia, pero, por el contrario, la actividad de los organismos e instituciones que se mueven en el marco del tercer pilar, como es el caso, por ejemplo, de las Autoridades de Control Comunes del SIS, SIA, Europol y Eurojust, queda fuera de su control.

[212] El TJCE es una institución única con dos jurisdicciones distintas, la del Tribunal de Justicia y la del Tribunal de Primera Instancia, siendo ambos órganos totalmente autónomos. Así, el TPI se ocupa entre otros asuntos de los litigios entre las Comunidades Europeas y sus funcionarios; de los recursos planteados por personas físicas o jurídicas contra la Comunidad; y de los recursos planteados por los Estados miembros y las instituciones comunitarias. Además, el TJCE le puede transferir todos los asuntos que le competen, con la excepción de las cuestiones prejudiciales.

[213] Pues la labor del TJCE consiste, exclusivamente, en interpretar las disposiciones comunitarias, sin sustituir al órgano jurisdiccional nacional, y corresponde al Juez nacional, ateniéndose a esa interpretación, elegir la manera de adecuar el ordenamiento jurídico de su país a las exigencias de la legislación comunitaria.

Los recursos que pueden presentarse ante el Tribunal de Justicia de las Comunidades Europeas son los siguientes:

El recurso de anulación:

El primer recurso que puede presentarse ante el TJCE es el recurso de anulación, cuyo objetivo es garantizar el respeto del Derecho comunitario por los propios órganos e instituciones comunitarios. Son impugnables los actos de las instituciones comunitarias que producen efectos jurídicos frente a terceros (Reglamentos, Directivas y Decisiones), no las normas comunitarias de Derecho originario (Tratados), ni las normas pertenecientes a ordenamientos jurídicos nacionales, por motivos de incompetencia, vicios sustanciales de forma, violación de los Tratados o de normas relativas a su ejecución y por desviación de poder. Por lo tanto, para que un acto sea recurrible en anulación la jurisprudencia comunitaria le exige que produzca efectos jurídicos obligatorios, que sea un acto definitivo y que no sea un acto de carácter interno de la Institución, sino que produzca efectos jurídicos para terceros.

El recurso por omisión:

Una segunda vía para controlar la legalidad de la falta de actuación de las Instituciones comunitarias y garantizar así, como en el caso anterior, el respeto del Derecho comunitario, la constituye el recurso por omisión[214].

Este recurso, complemento del anterior, se interpone ante el TJCE contra actos comunitarios y contra conductas, por lo que se podrá interponer contra Recomendaciones y Dictámenes. Pero

[214] Artículo 232 TCE (antiguo artículo 175): *"En caso de que, en violación del presente Tratado, el Parlamento Europeo, el Consejo o la Comisión se abstuvieren de pronunciarse, los Estados miembros y las demás instituciones de la Comunidad podrán recurrir al Tribunal de Justicia con objeto de que declare dicha violación. Este recurso solamente será admisible si la institución de que se trate hubiere sido requerida previamente para que actúe. Si transcurrido un plazo de dos meses, a partir de dicho requerimiento, la institución no hubiere definido su posición, el recurso podrá ser interpuesto dentro de un nuevo plazo de dos meses. Toda persona física o jurídica podrá recurrir en queja al Tribunal de Justicia, en las condiciones señaladas en los párrafos precedentes, por no haberle dirigido una de las instituciones de la Comunidad un acto distinto de una recomendación o de un dictamen. El Tribunal de Justicia será competente en las mismas condiciones para pronunciarse sobre los recursos interpuestos por el BCE en los ámbitos de sus competencias iniciados contra el mismo"*.

para poder interponerlo debe existir una inactividad inicial que siga subsistiendo tras haber requerido a la institución que actuara.

El recurso por omisión se puede interponer tanto por los Estados miembros y las instituciones comunitarias, como por los particulares, siempre y cuando *"no se les haya dirigido un acto distinto de una Recomendación o un Dictamen",* y se les podía haber dirigido. Las sentencias de los recursos por omisión se limitan a reconocer que la abstención de la institución es o no contraria al Derecho comunitario, pero no pueden adoptar el acto, ya que corresponde exclusivamente a la institución cuya omisión se haya declarado, adoptar las medidas necesarias para poner fin a la omisión.

La excepción de ilegalidad:

Otra posible vía para impugnar un acto comunitario de alcance general, aunque sin ser un procedimiento autónomo, es la excepción de ilegalidad. Es un procedimiento incidental que permite controlar, dentro del marco de un litigio principal en el que se impugna la aplicación de un acto de alcance general, la legalidad de dicho acto[215]. Esta vía supone una vía más accesible a los particulares que la del recurso de anulación, en tanto que puede ser utilizada por cualquiera de las partes de un litigio pendiente ante el TJCE. Además, aunque legalmente sólo se pueda interponer contra los Reglamentos, la jurisprudencia del TJCE ha admitido la posibilidad de impugnar todo acto de alcance general que constituya la base jurídica de la decisión atacada, aunque se exige que exista un vínculo directo entre la decisión atacada y el acto general cuya validez se cuestiona. La estimación de la sentencia no conlleva la nulidad del acto, sino su inaplicación. Es la institución que ha adoptado el acto declarado ilegal la que está obligada a adoptar las medidas que se derivan de la sentencia.

[215] Artículo 241 TCE (antiguo artículo 184): "Aunque haya expirado el plazo previsto en el párrafo quinto del artículo 230, cualquiera de las partes de un litigio en el que se cuestione un reglamento adoptado conjuntamente por el Parlamento Europeo y el Consejo o un reglamento del Consejo, de la Comisión o del BCE, podrá acudir al Tribunal de Justicia, alegando la inaplicabilidad de dicho reglamento por los motivos previstos en el párrafo segundo del artículo 230".

El recurso por incumplimiento:

Permite al Tribunal de Justicia controlar si los Estados miembros respetan las obligaciones que les incumben en virtud del Derecho comunitario. Antes de someter el asunto ante el Tribunal de Justicia tiene lugar un procedimiento previo dirigido por la Comisión, por el que se requiere al Estado miembro para que responda a las imputaciones de que ha sido objeto. Si tras este procedimiento el Estado miembro no ha puesto fin al incumplimiento, puede interponerse un recurso ante el Tribunal de Justicia por vulneración del Derecho comunitario.

Se puede plantear este recurso bien ante la Comisión[216], es el caso más frecuente en la práctica, o bien ante un Estado miembro. Si el Tribunal de Justicia declara que se ha producido un incumplimiento, el Estado de que se trate está obligado a adoptar sin demora las medidas necesarias para ponerle fin. Si después de serle sometido de nuevo el asunto por la Comisión el Tribunal de Justicia reconoce que el Estado miembro de que se trate no ha cumplido su sentencia, podrá imponerle el pago de una cantidad a tanto alzado o de una multa coercitiva. Así ocurrió, por ejemplo, en el caso *Comisión vs. Luxemburgo*, donde se condenó al Estado miembro por no haber cumplido con su obligación de transponer a su ordenamiento jurídico la normativa sobre protección de datos personales.

La acción de indemnización

Como consecuencia de los daños causados a los ciudadanos y a las empresas por las instituciones o agentes comunitarios en el ejercicio de sus funciones, se puede interponer ante el TJCE[217] la acción de indemnización o recurso por responsabilidad extracontractual.

---

[216] Artículo 226 TCE (antiguo artículo 169): "*Si la Comisión estimare que un Estado miembro ha incumplido una de las obligaciones que le incumben en virtud del presente Tratado, emitirá un dictamen motivado al respecto, después de haber ofrecido a dicho Estado la posibilidad de presentar sus observaciones. Si el Estado de que se trate no se atuviere a este dictamen en el plazo determinado por la Comisión, ésta podrá recurrir al Tribunal de Justicia*".

[217] Artículo 235 TCE (antiguo artículo 178): "*El Tribunal de Justicia será competente para conocer de los litigios relativos a la indemnización por daños a que se refiere el párrafo segundo del artículo 288*".

Esta acción se puede interponer por toda persona física o jurídica, así como por los Estados miembros, que consideren poseer un interés legítimo, es decir, que hayan sufrido el daño. Para solicitar la responsabilidad no basta que se declare la invalidez del acto, sino que se exige el concurso de un conjunto de requisitos en lo que se refiere a la ilegalidad de un acto de las instituciones, a la realidad del perjuicio y a la existencia de un vínculo de causalidad entre el acto y el perjuicio invocado.

Un claro ejemplo del ejercicio de esta acción lo encontramos en el caso *Stanley George Adams* en el cual se solicitó la compensación económica por los daños causados por la Comisión al desvelar cierta información sobre el demandante que podía dar lugar a su identificación. En este caso, se desestimó la acción interpuesta por no poder establecer la causalidad entre la acción de la Comisión y el perjuicio causado.

El recurso de casación

Para concluir, habría que señalar que contra las decisiones del Tribunal de Primera Instancia, que pueden ser consecuencia, por ejemplo, de un recurso de anulación, se puede interponer ante el TJCE un recurso de casación[218], aunque limitado a las cuestiones de Derecho. Si el recurso es admisible, el TJCE anulará la resolución del Tribunal de Primera Instancia.

Si el asunto lo permite, lo resolverá el TJCE, pero si no, se devolverá el asunto al Tribunal de Primera Instancia que estará vinculado por la decisión que se haya tomado en el recurso de casación. En el caso *Campogrande*, un particular solicitaba al TJCE un recurso de casación de una sentencia del Tribunal de Primera Instancia que había desestimado la anulación de una sanción de amonestación que le había impuesto la Comisión por no haber querido facilitarle sus datos domiciliarios. En este sentido, en el caso *X. vs. Comisión*, se recurrió en casación la sentencia del Tribunal de Primera Instancia que desestimaba la anulación de la decisión de la Comisión que le denegaba un puesto de trabajo, a

[218] Artículo 225 A TCE "…*Contra las resoluciones dictadas por las salas jurisdiccionales podrá interponerse ante el Tribunal de Primera Instancia recurso de casación limitado a las cuestiones de Derecho o, cuando la decisión relativa a la creación de la sala así lo contemple, recurso de apelación referente también a las cuestiones de hecho…*"

raíz de una prueba de detección del virus VIH que se le había realizado sin su consentimiento.

b) El Defensor del Pueblo Europeo:

El Defensor del Pueblo Europeo[219] ha desempeñado una labor muy importante en la protección de datos personales. En esta materia destaca el Informe Especial del Defensor del Pueblo al Parlamento Europeo en relación con la reclamación interpuesta por un particular, director de una empresa dedicada a la importación de cerveza alemana para su comercialización en el Reino Unido, ante la negativa de la Comisión de darle acceso a los alegatos llevados a cabo con motivo de una queja que el mismo había interpuesto ante la Comisión por considerar que la normativa sobre importación de cerveza en el Reino Unido era contraria a lo dispuesto en los Tratados.

También podemos citar la carta dirigida al Presidente de la Comisión, a finales del 2002, que se acompañó del documento *"El mal uso de las normas para la protección de datos en la Unión Europea",* en la que el Defensor solicitó que se clarificaran las normas comunitarias sobre protección de datos y propuso cambios en las mismas ante la creencia que se iba generalizando de que existía un derecho a participar de forma anónima en actividades públicas amparándose en la protección de datos personales[220].

B. Garantías específicas:

En el ámbito de la Unión Europea, el derecho a la protección de datos personales goza de un conjunto de garantías específicas. Tanto las Directivas sobre Protección de Datos como la normativa reguladora de los sistemas de información desarrollados en el marco del tercer pilar han establecido unos mecanismos de control

[219] El Defensor del Pueblo Europeo es un órgano previsto en el TCE que, igual que sus homónimos nacionales, está facultado para recibir las reclamaciones de cualquier ciudadano de la Unión o de cualquier persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, en los casos de "mala administración" por parte de las instituciones u órganos comunitarios, a excepción del TJCE o del TPI. El Defensor del Pueblo es un órgano independiente, que ejerce sus funciones con total independencia, y que actúa como mediador entre el ciudadano y la Administración comunitaria.

[220] M. ARENAS R., *El derecho fundamental a la protección de datos personales en Europa*, op. cit. p. 354 -355

de los tratamientos de datos personales que se lleven a cabo en la Unión Europea, incluso en el caso de que dicho tratamiento sea llevado a cabo por los organismos e instituciones de la Unión.

a) El Comité de protección de datos personales

En la Unión Europea la Comisión se ve asistida y tutelada en sus competencias de ejecución por Comités con diversas funciones. En materia de protección de datos personales también se ha creado un Comité de gestión encargado de asistir a la Comisión[221]. Este Comité, compuesto por representantes de los Estados miembros y presidido por el Presidente de la Comisión, tiene como función principal asesorar a la Comisión en materia de protección de datos personales, especialmente en las cuestiones relacionadas con la transferencia de datos. Es el Comité el que, a través de un Dictamen, indica a la Comisión la "adecuación" del nivel de protección ofrecido por un país tercero para que luego ésta decida incluirle en la "Lista blanca" de los países con los que la Unión Europea puede mantener intercambio de datos personales[222]. La Comisión informa a los ciudadanos de la labor de dicho Comité mediante la publicación de un Informe Anual y a través de la creación de un Registro de acceso público.

Este tipo de garantía no supone una garantía de acceso directo para los ciudadanos, pero a través del trabajo de esta Comisión se garantiza el cumplimiento de los requisitos para la protección de los tratamientos de datos personales, en concreto, los relativos a la transmisión de los mismos a Estados que no son miembros de la Unión.

b) El Grupo de Protección (El G 29):

Este grupo fue creado por la Directiva 95/46/CE sobre Protección de Datos Personales[223], con el fin de que los ciudadanos

[221] Artículo 31 de la Directiva 95/46/CE

[222] Considerando (66) Directiva 95/46/CE*: "Considerando que, por lo que respecta a la transferencia de datos hacia países terceros, la aplicación de la presente Directiva requiere que se atribuya a la Comisión competencias de ejecución y que se cree un procedimiento con arreglo a las modalidades establecidas en la Decisión 87/373/CEE del Consejo.4"*

[223] Considerando (65) Directiva 95/46/CE*:"Considerando que se debe crear, en el ámbito comunitario, un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, el cual habrá de ejercer sus funciones con plena independencia; que, habida cuenta*

pudieran acudir directamente a la Comisión ante las posibles vulneraciones que se produjeran en los tratamientos de sus datos personales en el ámbito comunitario, con la denominación de "Grupo de protección de las personas en lo que respecta al tratamiento de datos personales" (conocido como G 29), que actuase como intermediario, como "gran catalizador", entre las Autoridades de Control nacionales y la Comisión.

El G 29 está compuesto por un representante de la Autoridad o Autoridades de control designadas por cada Estado miembro, por un representante de la Autoridad o Autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión; de entre ellos se elige a su Presidente por un período de dos años renovable. De esta composición, así como de sus reglas de funcionamiento, se deduce el carácter consultivo e independiente del G 29, pues las Autoridades que lo componen no actúan sujetas a instrucción alguna por parte de sus respectivos Gobiernos[224]. El Órgano contribuye a la aplicación homogénea de las disposiciones nacionales que transponen las Directivas sobre Protección de Datos; asesora e informa a la Comisión sobre cualquier incidente en relación con la protección de datos personales, como, por ejemplo, sobre la existencia de divergencias entre la legislación y la práctica de los Estados miembros en esta materia; emite Recomendaciones sobre cualquier asunto relacionado con el tratamiento de datos personales, y Dictámenes sobre los códigos de conducta comunitarios y sobre el nivel de protección de datos existente dentro de la Comunidad y en los países terceros. De todas estas funciones destaca la elaboración de un Informe Anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, del que se da traslado al Parlamento Europeo, al Consejo y a la Comisión[225].

de este carácter específico, el grupo deberá asesorar a la Comisión y contribuir, en particular, a la aplicación uniforme de las normas nacionales adoptadas en aplicación de la presente Directiva";

[224] Artículo 29 de la Directiva 95/46/CE

[225] Artículo 30 de la Directiva 95/46/CE

c) El Supervisor Europeo de Protección de Datos:

La figura del Supervisor Europeo de Protección de Datos (SEPD) se creó en 2001 de conformidad con el artículo 286 del Tratado de la Comunidad Europea[226]. El SEPD tiene la responsabilidad de garantizar que las instituciones u organismos de la UE respeten el derecho de las personas a la intimidad en el procesamiento de sus datos personales. Cuando las instituciones u organismos de la UE procesan datos personales sobre una persona que pueda ser identificada, deben respetar el derecho de esa persona a la intimidad. El SEPD se asegura de que así se haga y les aconseja sobre todos los aspectos del procesamiento de los datos personales.

d) Las Autoridades Comunes de Control:

Los sistemas de información desarrollados a nivel europeo para la cooperación en materia policial y judicial, al no estar bajo el control directo del SEPD, han desarrollado una Autoridad de Control Común (ACC) encargada de garantizar la protección de datos personales en los tratamientos de datos que en ellos se realicen. Así, se ha creado una Autoridad de este tipo en el marco del SIS, del SIA, de Europol y de Eurojust. Aunque el Reglamento Eurodac también creó este tipo de Autoridad, cuando se creó el SEPD todas las funciones de la misma pasaron a ser asumidas por éste[227].

---

[226] Artículo 286 TCE: 1. *"A partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo.2. Con anterioridad a la fecha indicada en el apartado 1, el Consejo establecerá, con arreglo al procedimiento previsto en el artículo 251, un organismo de vigilancia independiente, responsable de controlar la aplicación de dichos actos comunitarios a las instituciones y organismos de la Comunidad y adoptará, en su caso, cualesquiera otras disposiciones pertinentes".*

[227] Art. 115 Convenio Schengen: "*1. Se creará una autoridad de control común encargada del control de la unidad de apoyo técnico del Sistema de Información de Schengen. Dicha autoridad estará compuesta por dos representantes de cada autoridad nacional de control. Cada Parte contratante dispondrá de un voto deliberativo. El control se ejercerá de conformidad con lo dispuesto en el presente Convenio, en el Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, teniendo en cuenta la Recomendación R (87) 15 de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa, dirigida a regular la utilización de datos de carácter personal en el sector de la policía y con arreglo al Derecho*

e) El Grupo de Berlín:

En 1983, a iniciativa de la Autoridad de Protección de Datos del *Land* de Berlín, se creó, en su seno, un Grupo de Trabajo dedicado a los problemas que el uso de las telecomunicaciones plantea en la vida privada de los individuos. A este Grupo se le conoce como "Grupo de Berlín". Este Grupo, compuesto por representantes de las Autoridades de control de un gran número de Estados, representantes de organizaciones internacionales públicas y privadas, y representantes de los sectores industriales implicados, todos ellos de la Unión Europea, se reúne cada cierto tiempo con el fin de debatir los problemas que las nuevas tecnologías y el uso de las telecomunicaciones provoca en el derecho a la protección de datos personales[228], e intentar buscar soluciones anticipándose a los problemas que se plantean en la práctica. De estas reuniones han surgido y surgen una multitud de Informes y Recomendaciones cuya finalidad es hacer frente a los problemas en los tratamientos de datos personales, cumpliendo así una función preventiva.

nacional de la Parte contratante responsable de la unidad de apoyo técnico. 2. Por lo que respecta a la unidad de apoyo técnico del Sistema de Información de Schengen, la autoridad de control común tendrá por cometido comprobar la correcta ejecución de las disposiciones del presente Convenio.
A tal fin tendrá acceso a la unidad de apoyo técnico. 3. La autoridad de control común también tendrá competencia para analizar las dificultades de aplicación o de interpretación que pudieran surgir con motivo de la explotación del Sistema de Información de Schengen para estudiar los problemas que pudieran plantearse en el ejercicio del control independiente efectuado por las autoridades de control nacionales de las Partes contratantes o en el ejercicio del derecho de acceso al sistema, así como para elaborar propuestas armonizadas con vistas a hallar soluciones comunes a los problemas existentes. 4. Los informes elaborados por la autoridad de control común se remitirán a los organismos a los cuales las autoridades de control nacional remitan sus informes".

[228] Su última reunión tuvo lugar en la capital alemana los días 5 y 6 de septiembre de 2006, con la presencia de más de cincuenta representantes de autoridades de control y expertos en protección de datos. Los participantes analizaron los posibles impactos de novedades tecnológicas y desarrollos jurídicos en el campo de las telecomunicaciones sobre el derecho fundamental a la protección de datos personales, en áreas tales como las redes de voz sobre Internet (VoIP), los servicios prestados a través de Internet (con especial atención a los motores de búsqueda y la telefonía IP), los servicios de administración electrónica (e-Government) y otros.

CONCLUSIONES FINALES:

1. El derecho a la autodeterminación informativa constituye uno de los más claros exponentes de los llamados derechos fundamentales de tercera generación, muy alejados de los primeros derechos reconocidos en el ámbito de las revoluciones burguesas, caracterizados por la defensa de la vida privada ante la intromisión de los poderes públicos, o de los de segunda generación para la salvaguarda de los aspectos económicos sociales y culturales. Las nuevas condiciones de ejercicio de los derechos humanos han determinado una nueva forma de ser ciudadano en el Estado de Derecho de las sociedades tecnológicas, lo cual justifica la inclusión de este derecho dentro de la tercera generación de derechos humanos.

2. Este nuevo derecho a la protección de los datos personales no supone reconocer a los titulares de los mismos un control absoluto sobre ellos. Pues ningún derecho tiene un carácter absoluto. Así los poderes públicos que integran la organización del Estado, para desempeñar diferentes tareas públicas que tienen atribuidas, necesitan indudablemente recoger y utilizar ciertos datos e informaciones de cada uno de los individuos que forman parte de la comunidad política.

3. El derecho a la autodeterminación informativa se diferencia acabadamente de los otros derechos como el derecho a la intimidad, pues éste último no responde a los criterios fundamentales precautorios que se observan en el objeto del derecho a la protección de datos personales. Esto, teniendo en cuenta que la función del derecho a la intimidad es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad; y la protección de datos personales garantiza a esa persona un poder de control sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del afectado. De forma que mientras el primero faculta que se excluyan del conocimiento de los demás los datos de alguien, el segundo garantiza un poder de disposición.

4. La creación tanto de garantías institucionales como individuales constituyen un claro ejemplo de las medidas que requiere la protección de datos personales y que van más allá del marco normativo del derecho a la intimidad, aunque éste último se encuentra también protegido a través de estas medidas. Podemos concluir entonces que es posible lograr la protección del derecho a la intimidad a través de la protección de datos, más no es posible lograr acabadamente la protección de datos personales a través de las garantías de un derecho meramente negativo como el de la intimidad.

5. El derecho a la autodeterminación informativa en el ordenamiento jurídico español se configura como un derecho fundamental autónomo e independiente. El reconocimiento del derecho fundamental a la autodeterminación informativa como derecho autónomo permite una mayor efectividad garantista, ya que si nos limitamos solo a tratar de salvaguardar los derechos de los ciudadanos a proteger sus datos personales con las herramientas jurídicas que devienen del derecho a la intimidad, no estaremos amparando el aspecto preventivo característico del derecho a la autodeterminación informativa, el cual no se contempla en la defensa del derecho a la intimidad, que más bien tiene un alcance meramente indemnizatorio para la víctima del agravio. Es necesario proveer al individuo de facultades que van más allá del la simple búsqueda del resarcimiento económico, otorgarles también instrumentos de actuación que les permitan a los titulares de controlar y determinar el destino u otros aspectos del tratamiento de sus datos personales.

6. El reconocimiento de este derecho como un derecho fundamental autónomo ha permitido un mayor desarrollo legislativo y a través de ello ha generado iniciativas que dieron nacimiento a la regulación pertinente y con ella los mecanismos que otorgan las suficientes garantías a los individuos, y que sirven de base para tutelar intereses de la persona tales como la dignidad, la libertad personal o el desarrollo de la personalidad, fines que persiguen también otros derechos fundamentales ya reconocidos y que al guardar tan estrecha relación con el derecho a la autodeterminación informativa, no hacen más que confirmar la condición de derecho fundamental de éste último.

7. El derecho a la autodeterminación informativa es un derecho fundamental reconocido a toda persona, independientemente de su condición de ciudadano, es decir, ha de garantizarse de forma equivalente para toda persona independientemente de su nacionalidad. Especialmente si se atiende a lo dispuesto en el artículo 13 de la Constitución Española que al regular los derechos de quienes no disfrutan la nacionalidad española dispone que: *"Los extranjeros gozarán en España de las libertades públicas que garantiza el presente Título en los términos que establezcan los Tratados y la Ley"*. Entre las libertades públicas que se garantizan en el Título I, destaca la limitación en el uso de la informática que, por lo tanto, ha de garantizarse de forma equivalente tanto a españoles como a extranjeros.

8. Las Recomendaciones de la OCDE, constituyen documentos orientativos de la actividad de los Estados miembros de esta organización, sin perjuicio de la recomendación que los mismos contienen de cumplir los principios establecidos en esos textos, su principal motivo fue la preocupación que algunos países, especialmente Estados Unidos, mostraban ante las iniciativas nacionales que iban surgiendo sobre protección de datos y el temor a que la regulación de esta materia creara barreras proteccionistas en el comercio internacional, no obstante, tienen por objeto el establecimiento de una regulación básica de protección de datos que garantice el libre flujo de la información entre los Estados participantes, lo cual constituyó un importante avance en esta materia.

9. La ratificación por parte de España, con fecha de 27 de enero de 1984 del Convenio 108 ha tenido una importante incidencia en el sistema jurídico Español. Esto se ve justificado constitucionalmente, ya que por imperio del artículo 96.1 de la CE de 1978, los Tratados internacionales válidamente celebrados, una vez publicados oficialmente en España, formarán parte del ordenamiento interno. Cumplidos ambos requisitos, el texto del Convenio Europeo, forma parte del sistema jurídico español, y hasta el año 1982, constituyó la norma básica en materia de protección de datos personales frente a los abusos cometidos en su procesamiento informático, lo cual significó un avance positivo en materia de protección de datos para el ordenamiento español.

10. La Directiva 95/46/CE de protección de datos, constituye el antecedente de la actual legislación, y delimita sin duda un marco regulador de protección de datos personales ineludible para el legislador español. Según ésta normativa, los Estados miembros se comprometen a garantizar "la protección de las libertades y los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales". Con respecto a ello, cabe destacar que la Directiva no reduce su objeto a la tutela de la intimidad, sino que se refiere a la protección de libertades y derechos fundamentales de las personas físicas, por lo tanto su protección no ampara a las personas jurídicas, sin embargo esto no coarta la libertad de los Estados Parte de ampliar el derecho a la protección de datos de carácter personal a las personas jurídicas.

11. El objeto de la LOPD es garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal. A través de la limitación del tratamiento de los datos de carácter personal, primer objeto de protección en la Ley, se intenta conseguir la salvaguardia de esa esfera de la libertad de las personas que se denomina autodeterminación informativa o libertad informática. Por lo tanto la finalidad de la Ley no es proteger los datos personales de los ciudadanos, sino la protección de éstos en relación con el tratamiento de los mismos, para salvaguardar en último término la libertad de la persona y posibilitar su desarrollo sin interferencias**.**

12. En lo que respecta a los titulares del derecho a la autodeterminación informativa, es menester considerar que tanto las personas físicas como jurídicas pueden tener interés en ejercitar el derecho de acceso, de rectificación o de cancelación de datos inexactos, falsos o desfasados, y si las personas de existencia ideal tienen la potestad de ejercer su derecho de rectificación ante los medios de comunicación, también deberían tener la facultad para reclamar el acceso, rectificación o cancelación de sus datos de carácter personal. Este reconocimiento del derecho a la autodeterminación informativa a las personas jurídicas se ve justificado, en que éstas tal como las personas físicas, tienen interés en obtener rectificación de sus datos equivocados que

figuran en ficheros públicos y privados, y por ello debe disponer de los medios jurídicos para ejercer sus derechos.

13. No cabe aplicar la Ley 15/1999 Orgánica de Protección de Datos de Carácter Personal a las personas fallecidas, lo cual se debe a la naturaleza misma del derecho protegido por la norma, teniendo en cuenta que la muerte de las personas da lugar a la extinción del derecho a la protección de sus datos personales, basado en el artículo 32 del Código Civil. Sin embargo, los familiares del causante podrán acudir a la instancia ordinaria, pero en defensa de los derechos establecidos en la Ley 1/1982 Orgánica de de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pero las personas legitimadas por la Ley 1/1982 carecerán de legitimación para el ejercicio de los derechos reconocidos por la LOPD, salvo en los supuestos en que esos derechos se ejerciten como instrumento para la realización de alguna de las finalidades protectoras indicadas que la Ley Orgánica 1/1982 les atribuye.

14. Los derechos que forman parte del contenido esencial de la protección de datos son independientes, y el ejercicio de ninguno de ellos es requisito previo para el ejercicio de otro derecho. Los derechos que reconoce al ciudadano la Ley 15/1999 le garantizan una defensa legal de su derecho a la protección de datos personales. Esta norma también impone al responsable del fichero deberes jurídicos, así como también a las demás personas que intervengan en alguna fase del tratamiento. Todo ello sirve para hacer realidad los principios de protección de datos y garantizar a las personas un control efectivo sobre sus datos personales.

15. Ante una violación del derecho a la protección de datos personales el titular de los mismos puede acudir a la vía judicial ordinaria, dependiendo del tipo de vulneración cometida frente al derecho a la protección de datos personales, además del recurso contencioso-administrativo que pueda interponerse frente a las decisiones de la Agencia Española de Protección de Datos, cabe acudir a la vía civil o penal.

16. El derecho de indemnización del daño moral no puede desconocerse porque el interesado tenga reconocidos otros derechos de defensa frente al tratamiento de sus datos, como el

derecho de oposición, rectificación o cancelación de los datos. Se trata de derechos diferentes, unos intentan prevenir utilizaciones ilícitas de los datos, y el otro pretende resarcir un incumplimiento del que sea ha derivado un perjuicio para el interesado.

17. La Agencia estatal es el eje vertebrador del sistema de protección de datos, asegurando por igual a todas las personas el contenido del derecho, de forma que se eviten discriminaciones por razones territoriales, pues lo contrario supondría lesionar el principio de igualdad en la titularidad del derecho fundamental de protección de datos. En cualquier caso, tanto el control de las Agencias Autonómicas en lo que se refiere al cumplimiento de la normativa sobre protección de datos, como la posibilidad de convocarlas a efectos de cooperación institucional, queda a discreción del Director de la AEPD.

18. Con respecto al carácter y naturaleza de la AEPD, ésta supera ciertos parámetros de independencia, especialmente en lo que se refiere al punto de vista funcional, normativo y financiero, es importante reconocer que el nombramiento y cese del Director depende del Gobierno y que la Memoria se presenta ante el Ministro de Justicia y no ante las Cámaras. Estas dos últimas circunstancias condicionan también la independencia de la institución, por lo que hubiese sido deseable que el legislador hubiera subsanado en la LOPD estos aspectos específicos.

19. La AEPD dispone de significativas facultades normativas en el régimen de aplicación y de desarrollo de la legislación de protección de datos, informando los proyectos de disposiciones generales que desarrollen esta legislación. La Agencia cuenta con potestad normativa propia, mediante instrucciones y recomendaciones con la finalidad de adecuar los tratamientos automatizados a los principios de la Ley. En su estructura pueden distinguirse dos tipos de órganos, unos de carácter ejecutivo y otro cuya función es la de asesoramiento. El primer grupo está formado por el Director de la Agencia, el Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General. El Consejo Consultivo es el órgano asesor.

20. Se debe reconocer la importante iniciativa por parte de la AEPD, de impulsar las vías de colaboración internacional con

Iberoamérica, entendiendo que el nacimiento de esa área geográfica y cultural al derecho a la protección de datos de carácter personal debería producirse desde la perspectiva de un intercambio global de experiencias puestas en común desde los diferentes ámbitos de decisión. Esta iniciativa dio origen a la Red Iberoamericana de Protección de Datos, órgano internacional compuesto por miembros de los países iberoamericanos, el cual que tiene por función reforzar la mutua y continua colaboración entre ellos en lo que respecta a la protección de datos de carácter personal.

21. Las Agencias autonómicas, son entes de derecho público "independientes", al igual que la estatal; no responden a órdenes, instrucciones ni a directrices administrativas. Su estructura orgánica es similar a la de la Agencia Española de Protección de Datos y se encuentran compuestas por un Consejo Consultivo, un Director y un Registro de Ficheros de Datos Personales, dependiente del Director. Las Agencias Autonómicas de Protección de Datos tienen las mismas competencias que la estatal, a excepción, como dice el artículo 41 LOPD, de las competencias relacionadas con las transferencias internacionales de datos, la publicidad de los tratamientos y la redacción de una Memoria Anual.

22. En el ámbito del Consejo de Europa, la principal garantía es el TEDH, al que se puede acudir agotada la vía judicial nacional para denunciar una violación del derecho a la protección de datos. Además existen también un Comisario para los derechos humanos y Comités independientes de estudio, así como un Grupo de Expertos y un Comité especializado sobre protección de datos.

23. En el ámbito de la Unión Europea el derecho a la protección de datos personales queda protegido por las garantías genéricas comunes a todos los derechos: el TJCE, ante el que se pueden presentar diferentes tipos de recursos, pero ninguno específico para la protección de los derechos fundamentales, y el Defensor del Pueblo Europeo. Además, el derecho a la protección de datos goza también de ciertas garantías específicas entre la que se destaca el Supervisor Europeo de Protección de Datos, autoridad independiente encargada de controlar los tratamientos de datos

personales efectuados en el campo de aplicación del Derecho comunitario.

BIBLIOGRAFÍA:

APARICIO SALOM, J. *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Navarra, 2000.

ARENAS RAMIRO, M. *El derecho fundamental a la protección de datos personales en Europa*. Agencia Española de Protección de Datos, Tirant lo Blanch, Valencia, 2006.

BALLESTEROS MOFFA, L. A. *La privacidad electrónica, Internet en el centro de protección*, Agencia Española de Protección de Datos, Tirant lo Blanch, Valencia, 2006.

CANALES GIL, A. *La Agencia Española de Protección de Datos: Estructura y Funcionamiento*, II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. 2ª Edición Protección de datos de carácter personal en Iberoamérica, Tirant lo Blanch, Valencia, 2006.

COLLADO GARCÍA-LAJARA, E. *Protección de datos de carácter personal, legislación, comentarios, concordancias y jurisprudencias,* Comares, Granada, 2000.

CORRIPIO GIL-DELGADO, M. *El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones,* Agencia Española de Protección de Datos, De Arellano, Madrid, 2001.

CUEVA CALABIA, J. L *La LORTAD y la seguridad de los sistemas automatizados de datos personales, en la Actualidad Informática* Aranzadi, número 13, octubre, Aranzadi, 1994.

DARANAS PELÁEZ, M. (Trad.) *Jurisprudencia constitucional extranjera. Tribunal Constitucional Alemán,* Ley del Censo, BJC, núm. 33, 1984.

DAVARA RODRÍGUEZ, M. A. La protección de datos en Europa. Principios, derechos y procedimiento, ASNEF-EQUIFAX Madrid, 1998.

DE LUCAS, J. *El concepto de solidaridad*, Fontamara, México, 1993.

FREIXAS GUTIÉRREZ, G. *La protección de los datos de carácter personal en el derecho español*, Bosch, Barcelona, 2001.

FROSINI, V. *Cibernética, derecho y sociedad*, Tecnos, Madrid, 1982.

GARCÍA-BERRIO HERNÁNDEZ, T. *Informática y libertades, la protección de datos personales y su regulación en Francia y España*, Colección de estudios de derecho, Universidad de Murcia, Murcia, 2003.

GARRIDO GÓMEZ, M. I. *Derechos fundamentales y Estado social y democrático de derecho*, Dilex, Madrid, 2007.

GARRIGA DOMÍNGUEZ, A. *La protección de los datos personales en el derecho español,* Dykinson, Madrid, 1999.

- *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid, 2004.

GRIMALT SERVERA, P. *La responsabilidad civil en el tratamiento de automatizado de datos personales*, Colección Estudios de Derecho Privado, núm 8, Granada, 1999.

HEREDERO HIGUERAS, M. *La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*, en Jornadas sobre "Informática Judicial y Protección de Datos Personales", celebradas en San Sebastián el 7 y 8 de octubre de 1993, Departamento de Justicia del Gobierno Vasco, Victoria- Gasteiz, Servicio Central de Publicaciones, 1994.

- La Agencia de Protección de Datos, Informática y Derecho, Nº 6-7, UNED, Mérida, 1994.

HERNANDO COLLAZOS, I. *La Comunidad Económica Europea y la informática.* Jornadas Internacionales sobre Informática y Administración Pública, Instituto Vasco de Administración Pública, Volumen 3, VVAA, Bilbao, 1986.

HERRÁN ORTIZ, A. I. *La violación de la intimidad en la protección de datos personales*, Dykinson, 1999.

-. *El derecho a la protección de datos personales en la sociedad de la información*, Universidad de Deusto, Instituto de Derechos Humanos, Cuadernos Deusto de Derechos Humanos, Núm 26. Bilbao, 2003.

- *Los derechos de las personas en la Ley Orgánica 15/1999, de 13 de diciembre de diciembre, de Protección de Datos de Carácter Personal.* En los XVII Encuentros sobre Informática y Derecho 2002-2003. Universidad de Comillas, Madrid, Facultad de Derecho, Instituto de Informática Jurídica, 2003.

HERRERO-TEJEDOR, F. *Honor, intimidad y propia imagen*, Colex, Madrid, 1994.

LÓPEZ RAMÓN, F. *La Agencia de Protección de Datos como Administración independiente*, en Jornadas sobre el Derecho Español de la Protección de Datos Personales, Agencia de Protección de Datos, Madrid, 1996.

LUCAS MURILLO DE LA CUEVA, P. *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990.

- *Informática y protección de datos personales*. Cuadernos y Debates Nº 43, Centro de Estudios Constitucionales, Madrid, 1996.

- "*Las funciones de la Agencia de Protección de Datos",* en Jornadas sobre el Derecho Español de la Protección de Datos Personales, Agencia de Protección de Datos, Madrid 1996.

- *La protección de datos en la Administración de Justicia*, Derecho a la intimidad y las nuevas tecnologías, Cuadernos de Derecho Judicial IX, Consejo General del Poder Judicial, Madrid, 2004.

MIERES MIERES, L. J. *Intimidad personal y familiar. Prontuario de jurisprudencia constitucional*, Editorial Aranzadi, S.A. Navarra, 2002.

NAVALPOTRO NAVALPOTRO, Y. VV.AA. *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, Valladolid, 2005.

OROZCO PARDO, G. *Consideraciones sobre los derechos de acceso y rectificación en el proyecto de ley orgánica de regulación de datos de carácter personal*, Informática y Derecho, nº 6-7, 1994.

ORTÍ VALLEJO, A. *Derecho a la intimidad e informática. Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada*, Granada, Comaraes 1994.

PÉREZ LUÑO, A. E. *Nuevos derechos fundamentales de la era tecnológica: la libertad informática*, ADPEP. núm. 2., 1989.

- *Los derechos humanos en la sociedad tecnológica*, Libertad informática y leyes de protección de datos, Cuadernos y Debates 21, Centro de Estudios Constitucionales, Bilbao, España, 1989.

- *Los derechos humanos en la sociedad tecnológica*, en Losano M. y otros: Libertad informática y leyes de protección de datos, Centro de Estudios Constitucionales, Madrid, 1990.

- *Perfiles morales y políticos del derecho a la intimidad*, en Anales de la Real Academia de las Ciencias Morales y Políticas, año XLVIII, número 73, Madrid, 1996.

- *Manual de Informática y Derecho,* Ariel, Barcelona, 1996.

- *La tutela jurídica de los datos personales en España,* en la Toga, nº 131, Ilustre Colegio de Abogados de Sevilla, diciembre de 2001.

-. *Derechos Humanos, Estado de Derecho y Constitución*, octava edición, Tecnos, Madrid, 2003.

- *La tercera generación de derechos humanos*, Aranzadi, Navarra. España, 2006.

PUENTE ESCOBAR, A. *Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal.* II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003. 2ª Edición Protección de datos de carácter personal en Iberoamérica, Tirant lo Blanch.Valencia, 2006.

RODRÍGUEZ PALOP, M. E. *La nueva generación de derechos humanos*, Dykinson, Madrid, 2002.

RUIZ MIGUEL, C. *En torno a la protección de los datos personales automatizados*. Revista de Estudios Políticos (Nueva Época), num. 84 abril – junio. 1994.

- *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*, Cuadernos Civitas, Madrid, 1994.

SANCHO VILLA, D. *Transferencia internacional de datos personales*, Agencia Española de Protección de Datos, De Arellano, Madrid, 2003.

VASAK, K. *Diferentes catégories des droits de I´homme*, en LAPEYRE, A., DE TINGUY, F. y VASAK, (Dir.): Les dimensions universelles des droits de I´homme, Bruylant, Bruxelles, 1990.

VIGGIOLA, L.E. y MOLINA QUIROGA, E. *Tutela de la autodeterminación informativa. Aproximación a una regulación eficaz del tratamiento de datos personales*. Ponencia presentada al Congreso Internacional "Derechos y Garantías en el Siglo XXI" de la Asociación de Abogados de Buenos Aires. Documento electrónico localizado en http://www.aaba.org.ar/bi151302.htm. Abril de 1999.

WARREN, S. y BRANDEIS, L. *The Right to Privacy*, Civitas, 1995.

DOCUMENTACIÓN UTIZADA:

Jornadas sobre protección de la privacidad, telecomunicaciones e Internet, Pamplona 22 y 23 de junio de 2000. Agencia de Protección de Datos. Universidad Pública de Navarra.

Derechos Humanos y nuevas tecnologías, Jornadas sobre Derechos Humanos núm. 6, XXI Cursos de Verano en San Sebastián, XIV Cursos Europeos, UPV/EHU, Ararteko, País Vasco, 2002.

La Red Iberoamericana de Protección de Datos, Declaraciones y Documentos, Agencia Española de Protección de Datos, Tirant lo Blanch, Valencia, 2006.

Guía del Derecho Fundamental a la Protección de Datos de Carácter Personal, Agencia Española de Protección de datos, Madrid, 2004.

Memorias de la Agencia Española de Protección de Datos, desde el Año 1994 al Año 2005.

ABREVIATURAS:

AEPD: Agencia Española de Protección de Datos

CE: Constitución Española

CEDH: Convenio Europeo de Derechos Humanos

EAEPD: Estatuto de la Agencia Española de Protección de Datos

G 29: Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, creado por la Directiva 95/46/CE sobre Protección de Datos Personales.

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

LORTAD: Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos Personales

OCDE: Organización para la Cooperación y Desarrollo Económico

RD: Real Decreto

STC: Sentencia del Tribunal Constitucional

STEDH: Sentencia del Tribunal Europeo de Derechos Humanos

STS: Sentencia de Tribunal Supremo

TEDH: Tribunal Europeo de Derechos Humanos

TJCE: Tribunal de Justicia de las Comunidades Europeas

UE: Unión Europea

3.- JURISPRUDENCIA

JUZGADOS DE PRIMERA INSTANCIA

JUICIO: "C. R. B. C. s/HABEAS DATA".-

ACUERDO Y SENTENCIA NÚMERO: cincuenta y cuatro

Asunción, 09 de mayo de 2002.-

VISTA: La presente acción de Habeas data de la que.-

R E S U L T A:

Que en fecha 05 de marzo del te año, se presentó el Abogado C. R. B. C. a promover acción constitucional de Habeas Data contra la Dirección de Identificaciones de la Policía Nacional, basado entre otras cosas en las siguientes términos: "…que en fecha 2 de marzo del año en curso se publicaron profusamente en el diario ABC Color … supuestos antecedentes penales que obran contra mi personas en los archivos de la Policía de Identificaciones, con la finalidad de hacerme aparecer ante la opinión pública como un abogado criminal que defiende a criminales … Hace varias años se promovieron algunas querellas criminales contra mi persona ... Las mismas han sido sobreseídas en su totalidad, habida cuenta de sus abiertas improcedencias y mala fe… todas las resoluciones favorables en su totalidad a mis derechos, han sido remitidas en su oportunidad a la Policía Nacional, a fin que se proceda a la destrucción de aquellos antecedentes registrados, que en su momento constituían antecedentes de causas penales en tramite… los archivos de la Policía Nacional no son públicos para nadie y sólo se pueden acceder a los mismos, por disposición judicial… la policía de identificaciones al expedir informaciones reservadas y confidenciales, mercan con la personalidad de terceros, siendo esta una violación a la Constitución Nacional que la turba, violenta y la pone en permanente jaque en su art. 33.." Termina solicitando se requiera a la Dirección de Identificaciones que informe al Juzgado en relación a si obran en sus archivos, antecedentes policiales y judiciales referentes a los hechos relativos a su personalidad y en caso positivo, que remita al Juzgado dichos antecedentes, debiendo aclarar al mismo tiempo el uso que dan de ellos y su finalidad que una vez constatados de que esas informaciones afectan ilegalmente

a mis derechos constitucionales, ordenara la destrucción de los mismos.-

Que el Juzgado por providencia de fecha 11 de marzo del corriente año, tuvo por presentado al recurrente en el carácter invocado y por constituido su domicilio en el lugar señalado. Igualmente dio inicio a la presente acción de Habeas Data que promueve el Sr. C. R. B. Cárdenas contra la Dirección de Identificaciones de la Policía Nacional y corrió traslado a la demandada citando y emplazándola para que en el perentorio término de cinco días conteste la demanda.-

Que a fs. 49 de autos, obra el informe remitido por el Jefe del Departamento de Identificaciones a través del cual arrimó al Juzgado fotocopias del prontuario de antecedentes penales correspondientes.-

Que el Juzgado por providencia de fecha 05 de abril del corriente año, agregó las instrumentales presentadas por el Jefe de Identificaciones de la Policía Nacional y por providencia de fecha 07 del mes de mayo del corriente año, habiendo sido evacuado el informe pertinente y recaudos requeridos y no habiendo pruebas que diligenciar, el Juzgado llamó Autos para Sentencia, y

C O N S I D E R A N D O:

Que la pretensión del actor del presente Habeas Data consiste en: "…acceder a los archivos de la Policía de Identificaciones de la Policía Nacional… que informe al juzgado en relación si obran en sus archivos, antecedentes policiales y judiciales referentes a los hechos relativos a mi personalidad, y en caso positivo, deberá remitir al juzgado dichos antecedentes, debiendo aclarar al mismo tiempo el uso que dan de ellos y su finalidad, que una vez constatados de que esas informaciones afectan ilegalmente a mis derechos constitucionales, ordenará V.S., la destrucción de los mismos, por ser de estricta justicia constitucional". El accionante explica que en fecha 02 de marzo de 2002 se publicaron en el Diario ABC COLOR, supuestos antecedentes penales que obran en contra su persona en los archivos de la Policía de Identificaciones con la

finalidad de hacerle aparecer como un "abogado criminal que defiende a criminales" constituyendo dicho hecho una intromisión en su vida privada y profesional, más adelante reconoce que años atrás había sido sujeto de querellas criminales en su calidad de Presidente de la firma Global S.A. aclarando que las mismas han sido sobreseídas en su totalidad; también menciona que las querellas que se le iniciaron fueron a raíz de una homónima con un tal C. B. quien había sido un nefasto personaje de épocas pasadas. -

Por su parte la Policía, a través del Departamento de Identificaciones, contestó según documentos obrantes a fs. 36 a 79 de autos, manifestando que el Sr. C. B. C. no registra antecedentes y remite fotocopia del prontuario de antecedentes penales y los oficios correspondientes de cada una de las causas mencionadas en dicho prontuario. -

La presente causa debe ser analizada a la luz del art. 135 de la Constitución Nacional el cual reza: "Toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad, Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, se fuesen erróneos o afectaran ilegítimamente sus derechos". Ahora bien el objeto de la presente acción de Habeas Data ya ha sido parcialmente cumplido, efectivamente el recurrente solicitó acceder a los archivos de la Policía y para ese efecto requirió que esa institución informara si obran en su poder antecedentes policiales y judiciales referentes a hechos que se le atribuyen a su persona y en caso afirmativo que remita dichos antecedentes; como se dijera líneas más arriba el Departamento de Identificaciones remitió fotocopia del prontuario del actor proporcionando los datos requeridos por el mismo.-

Ahora bien, en lo referente a la pretensión del demandante de que se ordene la destrucción de los antecedentes que sobre su persona obren en la repartición pública señalada, la misma carece de fundamento jurídico puesto que el art. 135 de la Carta Magna dispone que la "actualización, la rectificación o la destrucción" de los datos procede cuando los mismos sean erróneos o afectaren

ilegítimamente a los derechos del recurrente. En el caso de autos el demandante no demostró que los antecedentes que sobre su persona obran en la Policía sean erróneos o desactualizados; y en cuanto a que dañen ilegítimamente a sus derechos, cabe acotar que lo que eventualmente perjudicaría al recurrente es la publicación parcial de que tales datos se hiciera en un diario del país, mas no los antecedentes en sí, los cuales deben obrar en los archivos oficiales (en este caso del Departamento de Identificaciones de la Policía Nacional). Efectivamente, ésta informó que el recurrente "no registra antecedente", ello debido a que las causas judiciales que se le formaron al actor fueron finiquitadas ya sea por prescripción o por extinción, según el informe remitido por la Policía. El accionante deberá recurrir a las vías legales idóneas correspondientes a fin de determinar quines son los responsables de la publicaciones que dice afectan ilegítimamente a su vida privada y dignidad para así obtener el resarcimiento correspondiente.-

POR TANTO en mérito a las consideraciones expuesta y a la disposiciones legales citadas, el Juzgado.-

R E S U E L V E:

1) HACER LUGAR PARCIALMETNE, a la acción de HABEAS DATA promovida por C. B. C. conforme a los argumentos esgrimidos en el considerando.-

2) IMPONER las costas en el orden causado.-

3) ANOTAR, registrar y remitir copia a la Excma. Corte Suprema de Justicia.

Firmado: Alma Mendez de Boungermini, Jueza
Ante mí: Arnaldo Alvarez Figueredo, Actuario Judicial.

JUICIO: "P. M. F. C/MINISTERIO DE EDUCACIÓN Y CULURA S/HABEAS DATA".-

S.D. N^{O} 53

VISTOS: La presente acción de Habeas Data de la que-

R E S U L T A:

Que en fecha 26 de noviembre de 2004, se presentó ante este Juzgado P. M. F. por derecho propio y bajo patrocinio de abogado, a promover juicio de hábeas data contra el Ministerio de Justicia y Trabajo, manifestando entre otros puntos: "… vengo a solicitar al Juzgado a cargo de V.S., esta petición como me comunicaron que ya habían salido mis rubros como docente ante el dicho Ministerio como estoy enseñando en la Escuela Básica María Auxiliadora Nº 3638 Zona 2 Canindeyu Distrito de Yasy Kañy, más de tres años como Ad Honoren, me presente ante el Ministerio de Educación y Cultura, no me quisieron dar ninguna respuesta. Por tanto vengo a solicitar esta petición para que informe a éste Juzgado con relación de los mencionado expuesto más arriba…".-

Que el Juzgado por providencia de fecha 02 de diciembre de 2004, tuvo por iniciada la demanda que promueve el Sr. P. M. F. contra el Ministerio de Educación y Cultura y de la misma corrió traslado a la parte demandada por el plazo dispuesto por ley.-

Que en fecha 15 de abril de 2005, se presentó ante el domicilio particular del Actuario el Abogado W. S. C. en representación del Ministerio de Educación y Cultura, a contestar el traslado corrídole manifestando entre otros puntos: "…la parte actora falta a la verdad al expresar que el habían comunicado que le han asignado rubros como docente y que se ha constituido hasta las oficinas del Ministerio de Educación y Cultura ha solicitar información y no obtuvo ninguna respuesta …LA VERDAD de los hechos es que el actor de la presente acción se halla incorporado al Magisterio Nacional, como Docente y Catedrático en los siguientes cargos. Un (1) Rubro de Categoría LOG, así como en 40 (Cuarenta) Horas Cátedras, de la Categoría Z43, en la Escuela Graduada N^{o} 3638

"María Auxiliadora del Distrito de Yasy Kañy, Región Nº "4" Canindeyú, tal como surge del informe elevado por la Lic. D. S., Directora General de la Dirección de Gestión Escolar Administrativa, a través de Memorando Nº 155 fe fecha 15 de abril de 2005, donde igualmente se halla acompañados el Certificado de Trabajo del citado Docente y Cuadro de Personal donde se colige que el citado educador se halla cumpliendo sus funciones en la Institución Educativa citada más arriba .. es oportuno hacer notar al Juzgado que el Ministerio de Educación y Cultura, en ningún momento ha obstruido o ha impedido el acceso a todas las documentaciones e informaciones que existen en los archivos de la Institución con relación al Prof. P. M. F.…".-

Que el Juzgado por providencia de fecha 21 de abril de 2005, tuvo por contestado el traslado en los términos del escrito presentado y no existiendo prueba que diligenciar en estos autos, llamó autos para sentencia.-

C O N S I D E R A N D O:

El actor P. M. F., por derecho propio y bajo patrocinio de abogado, alega que viene a promover la acción de Habeas Data a fin de que el Ministerio de Educación y Cultura informe si "… ya habían salido mis rubros como docente…" alegando que se encuentra trabajando "Ha Ornaren" en la escuela Básica Maria Auxiliadora desde hace más de tres años.-

Por su parte el demandado, Ministerio de Educación y Cultura, contestó el traslado señalando que el actor se encuentra incorporado al Magisterio Nacional como Docente y Catedrático en la Escuela Graduada Nº 3638 "María Auxiliadora" del distrito de Yasy Kañy, adjuntando el Memorando Nº 155/2005 de la Dirección General de Gestión Escolar Administrativa y la planilla de Cuadro de Personal de la citada escuela.-

En primer lugar es importarte acotar que del confuso escrito de inicio de la demanda, el cual orilla entre una acción de amparo de pronto despacho y la de habeas data, se interpreta que el actor desea que el Ministerio de Educación y Cultura le provea los

documentos donde se informa sobre "su rubro" dentro de la institución educativa María Auxiliadora del Distrito de Yasy Kañy, Canindeyú. La pretensión del mismo debe ser estudiada a la luz del art. 135 de la Constitución Nacional el cual reza: "Toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos", así también deben considerarse las leyes reglamentarias Nº 1682/2001 y 1696/2002. La norma citada es sumamente clara y no caben dudas de que ampara plenamente al accionante, de hecho la demandada ha arrimado al Juzgado las instrumentaciones solicitadas por el demandante, por ende, no queda más que hacer lugar a la presente acción de Habeas Data. En cuanto a las costas, el Juzgado considera que corresponde imponerlas en el orden causado, dado que la demandada arrimó a autos los documentos solicitados por el accionante, además de no haber quedado demostrado que el Ministerio se haya negado a informar al accionante sobre lo peticionado. -

POR TANTO, de conformidad a las disposiciones legales citadas le Juzgado:-

R E S U E L V E:

1) HACER LUGAR a la acción de Habeas Data promovida por P. M. F. contra el MINISTERIO DE EDUCACIÓN Y CULTURA S/HABEAS DATA".-

2) IMPONER las costas en el orden causado.-

3) ANOTAR, registrar y remitir copia a la Excma. Corte Suprema de Justicia.- - - - - - -

Firmado: Alma Mendez de Boungermini, Jueza.
Ante mí: Arnaldo Alvarez Figueredo, Actuario Judicial.

JUICIO: "J. A. A. A. c/BANCO NACIONAL DE FOMENTO S/HABEAS DATA".-

ACUERDO Y SENTENCIA NÚMERO: CIENTO CUARENTA Y NUEVA.-

Asunción, 05 de Octubre de 2005.-

VISTO: El pedido de acción de Habeas Data promovida por JEAN ALAIN ADRIEN ATENEN, de los que:-

R E S U L T A:

QUE, a fs. 08 de autos se presentó ante el juzgado de la Niñez el Sr. J. A. A. A., a plantear la Acción de Garantía Constitucional de Habeas Data contra el BANCO NACIONAL DE FOMENTO.-

QUE, a fs. 10 de autos, el Juzgado dictó el A.I.Nº 278 de fecha 11 de julio de 2005, en el que se resolvió correr traslado del Habeas Data interpuesto a la parte demandada, el Banco Nacional de Fomento, citándola y emplazándola para que la conteste en el término de cinco (05) días (…)".-

QUE, a fs. 16/22 de autos, se presenta la parte demandada, el Banco Nacional de Fomento, y contesta el traslado corrídole, escrito mediante, representado convencionalmente por los Abogados V. M. C. R. y G. A. V. G.-

QUE, a fs. 23 de autos, el Juzgado resolvió por providencia de fecha 25 de julio de 2005 tenerlos por presentados a los recurrentes, y se corrió vista al Ministerio Público, Fiscalía General del Estado.-

QUE, a fojas 24 de autos obran el Dictamen Nº 222 de fecha 22 de setiembre de 2005, de la Fiscalía General del Estado, por el representante del Ministerio Público Abogado Diosnel Rodríguez, quien ostenta el cargo de Fiscal General Adjunto, y contesta la vista corrídole por esta Magistratura, en los términos del dictamen que precede.-

QUE, por providencia de fecha 26 de setiembre del año 2005 el Juzgado llamó a Autos para Sentencia, y;-

C O N S I D E R A N D O:

QUE, preliminarmente es fundamental delimitar la acción planteada ante este Juzgado y comprender su naturaleza jurídica. Nuestra Carta Magna, la Constitución Nacional del año 1992 preceptúa y regula la Garantía Constitucional de Habeas Data, atribuyéndole jerarquía y relevancia constitucional. -

QUE, ahora bien, nuestra Constitución en su art. 135 estipula lo siguiente: "Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad, podrá solicitar ante el Magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos".-

QUE, conforme se puede valorar, el Habeas Data constituye una acción que tiene como objetivo fundamental el acceso de las personas a los datos a ellas referidas, controlar su veracidad y rectificarlos o suprimirlos en casos de ser errados, incompletos o falsos, de donde se desprende que éste es un derecho constitucional reconocido, y la misma como garantía busca su efectiva protección ante dichas circunstancias.-

QUE, el actor, escrito mediante manifestó que: *"(…) por el presente escrito vento a solicitar Recurso Constitucional de Habeas Data (…) Que por resolución Nº 1, acta Nº224 de fecha 03 de diciembre de 1991, el Consejo de Administración del Banco Nacional de Fomento me ha otorgado un crédito de monto 88.000.000 Gs. De conformidad al: 1) Proyecto de inversión en la nota de fecha 11 de octubre de 1991 registrado bajo el Nº 2762 el 28 de noviembre de 1991; 2) Informe de fecha 25 de octubre de 1995 de la División de Estudios y Análisis del Departamento de Desarrollo; y, 3) Resolución Nº 01, Acta Nº 95 de fecha 01 de noviembre de 1995 del Consejo de Administración del Banco"*. Asimismo agregó que: *"Que, para*

proseguir trámites judiciales y administrativos necesito de una copia autenticada de las Resoluciones up supra mencionadas y de sus anexos (…)" (SIC).-

QUE, en su oportunidad procesal, la parte demandada contestó la demanda y expresó lo siguiente: *"En tiempo y forma oportunos, cumpliendo expresas instrucciones recibidas de mi principal, por medio del presente escrito vengo a contestar el traslado dispuesto por el Juzgado de Vuestra Señoría (…) haciéndolo en los siguientes términos (…) Los presupuestos establecidos en la Constitución para la procedencia de esta garantía constitucional son los siguientes:*

1) Debe tratarse de información sobre una persona o sobre sus bienes; (…)

2) La información debe constar en registros oficiales o privados de carácter público. Si bien el Banco Nacional de Fomento, es un entidad del Estado, el archivo existente en la Institución tiene como única finalidad la guarda de las documentaciones que allí son archivadas o depositadas. Siendo ésta su única finalidad, el acceso a las informaciones en ella archivadas se encuentran restringidas para terceras personas, por ende no susceptible de proveer informaciones a extraños en Relación BANCO – CLIENTE, dado el deber de secreto que rige a las entidades del sistema financiero (…) Con esto queda indudablemente aclarado, que los archivos del Banco Nacional de Fomento NO son de carácter público, como lo exige el art. 135 de la C.N. y por tanto insusceptibles de ser alcanzados por la Acción de Habeas Data".-

QUE, asimismo en virtud a la vista corrídole por el Juzgado, el Representante del Ministerio Público por medio del Dictamen Nº 111 dijo: *"En relación a los requisitos que cualquier petición de Habeas Data debe reunir son los siguientes: "Identificar el registro de que se trata; b) Expresar en que consiste la ilegalidad que afecta a sus derechos. Que la fundamentación dada por el recurrente a los efectos de utilizar esta vía, para la obtención de copias autenticadas de las resoluciones que se menciona en su petición, a los efectos de utilizarlos en procedimientos judiciales y administrativos, no condice con la naturaleza ni el objeto para lo cual se estableció esta garantía constitucional; por lo que es de parecer de esta*

representación fiscal, que no corresponde hacer lugar a dicha pretensión". (SIC).-

QUE, corresponde pues examinar si se configuran los extremos contemplados en el mando constitucional establecido en el art. 135 de la Constitución. Primeramente, y conforme a la interpretación extensiva que debe efectuarse en estos autos, la parte demandada en el presente juicio, la entidad pública crediticia y fomento, el Banco Nacional de Fomento (B.N.F.) no reviste o no configura en "Registro Oficial o Privado de datos o información de carácter público".-

QUE, asimismo, y teniendo en cuenta que entre las partes ha existido una relación jurídica contractual, en la cual el propio accionante ha proveído de datos en calidad de cliente, a la institución bancaria pública demandada, es del parecer de ésta Magistratura que la acción de Habeas Data impetrada, NO es el medio idóneo a los fines del recurrente constitucional.-

QUE, el Tribunal de Apelaciones de la Niñez y la Adolescencia de la circunscripción judicial de la Capital, en un caso judicial similar sobre Habeas Data, en un interesante y motivado fallo resolvió cuanto sigue: "(…) De acuerdo con la norma transcripta y analizándola desde el punto de vista lingüístico, necesariamente debe convenirse que la entidad demandada, en éste caso el Banco Sudameris, no es un registro oficial y tampoco un registro privado de carácter público. Por lo tanto, al no configurarse ninguno de estos requisitos básicos que determina la viabilidad de la acción e Hábeas Data, no podría sostenerse válidamente que tenga la legitimación pasiva para intervenir como parte accionada en el presente juicio, tal como lo resolvió el Juzgado por A.I. N° 452 del 5/11/01 (…)". (SIC) (Acuerdo y Sentencia N° 57 de fecha 25 de junio del 2003). -

QUE, la autorizada opinión de la tratadista argentina, Dra. María Mercedes Serra considera que *"(…) el Habeas Data es una garantía constitucional, cuyo objetivo primordial es la obtención de los datos relativos a una persona que obran en los registros públicos"*

(Reflexiones acerca del Habeas Data, en Boletín de la Asociación Argentina de Derecho Constitucional 1997, Nº 130, pág. 11.).-

QUE, coincidentemente con lo expresado por el representante del Ministerio Público, éste Juzgado no encuentra los requisitos necesarios para la procedencia de la garantía incoada

QUE, de conformidad a los fundamentos expuestos precedentemente, es criterio de ésta Magistratura imponer las costas a la parte perdidosa, de acuerdo al principio general de las costas establecidas en el art. 192 del Código Procesal Civil.-

POR TANTO, a mérito de las consideraciones expuestas el Juzgado de Primera Instancia de la Niñez y la Adolescencia del Segundo Turno de la Circunscripción Judicial de la Capital:-

R E S U E L V E:

1) NO HACER LUGAR, a la Acción constitucional de HABEAS DATA planteada por el Sr. J. A. A. A., contra el BANCO NACIONAL DE FOMENTO, en base a las consideraciones expuestas en el exordio de la presente resolución judicial.-

2) COSTAS, a la parte perdidosa.-

3) ANOTAR, registrar y remitir copia a la Excma. Corte Suprema de Justicia.-

Firmado: Maria Eugenia Giménez de Allen, Jueza.
Ante mí: Martín Muñoz Carman, Actuario Judicial.

JUICIO: "F. F. C. c/ POLICÍA NACIONAL S/HABEAS DATA".-

S.D. N° 74

VISTOS: La presente acción de habeas data de la que

R E S U L T A:

Que en fecha 09 de setiembre de 2005 se presentó el señor F. F. C., por derecho propio y bajo patrocinio del Abogado A. R. E., a promover acción de habeas data contra la Policía Nacional, en el escrito de fs. 18 de autos, manifestando entre otros puntos:"…he nacido en la República del Paraguay, en la ciudad de Coronel bogado, en fecha 02 de Abril de 1959, siendo mis padres los Señores F. F. y T. C., conforme así lo demuestro con el Certificado de Nacimiento expedido por el Registro del Estado Civil de las Personas … Desde el año 1963 residí en la ciudad de Buenos Aires, República Argentina, y desde el 1988 me radiqué finalmente en el Paraguay … a partir del año 2001 he tenido inconvenientes en cuanto a mis antecedentes orantes en los Registros de la Policía Nacional, concretamente en el Departamento de Identificaciones. Así, adjunto a esta presentación y ofrezco como prueba el Certificado de Antecedentes Policiales expedido en fecha 19 de Setiembre de 2001, en donde V.S. se percatará de que aparece lo siguiente: "REGISTRA ANTECEDENTE. 24/11/98. S/DELITO DE ABIGEATO. ROBO. ASALTO. POSESIÓN Y TENENCIA DE MARIHUANA CAPITAN BADO EXCMA. CORTE SUPREMA DE JUSTICIA LIBERTAD: EXCARCELACIÓN POR LIBERTAD CONDICIONAL O/MINISTRO PROF. DR. WILDO RIENZI GALENO. SRIA. FABIAN ESCOBAR DIAZ A.I. N° 1545 F: 23/11/98 …Corresponde aclarar que previo a dicha certificación, no he tenido ningún tipo de antecedentes, conforme así lo demuestro con el pertinente Certificado expedido en fecha 07 de Octubre de 1997.-

A raíz de la aparición de los antecedentes señalados precedentemente, en fecha 22 de Diciembre de 2003 he cursado Nota al Comisario Principal DAEP V. V. Z … en donde solicité la revisión de mis antecedentes policiales, advirtiendo de la usurpación de mi identidad por parte de otra persona, también

llamado F. F. C., quien aparentemente no posee Cédula de Identidad Policial Paraguaya, por lo que los antecedentes policiales y penales del mismo fueron cargados en mi prontuario, hasta el momento libre de todo registro … Como consecuencia de la nota presentada por mi parte en fecha 22 de Diciembre de 2003 fueron rectificados mis antecedentes y así de mi prontuario fueron "borrados" los delitos atribuidos a mí homonimia … Sin embargo, en fecha 09 de junio de 2005 acredita con las instrumentales agregadas a estos autos, se debería a la persistencia de los registros Antecedentes que eventualmente correspondería a un Homónimo, motivo por el cual, mi parte considera pertinente que antes de emitir Resolución, se disponga la comprobación de la existencia de otra persona quién eventualmente habría sido procesado en la causa debidamente individualizada en el apartado precedente según Oficio Nº 880 del 22 de mayo de 2002, remitida a la Comandancia de la Policía Nacional por el Juzgado Penal de Liquidación y Sentencia de la Circunscripción Judicial de Caaguazú y San Pedro, cuya fotocopia se acompaña…".-

Que por providencia de fecha 20 de octubre de 2005, se tuvo por reconocida la personería del recurrente en el carácter invocado, por constituido su domicilio en el lugar señalado y por contestada la demanda en los términos del escrito presentado. Como medida de mejor resolver libraron oficios a la Penitenciaría Regional del Amambay y al Departamento de Estadística Criminal de los Tribunales y a la Jueza Penal de Liquidación y Sentencia de la Circunscripción Judicial de Caaguazú y San Pedro. Por providencia de fecha 15 de junio de 2006, habiéndose dado cumplimiento al proveído de fecha 20 de octubre de 2005, y no existiendo prueba pendiente de diligenciamiento, se llamó AUTOS PARA SENTENCIA, y -

C O N S I D E R A N D O:

El actor F. F. C. se presenta, por derecho propio y bajo patrocinio de Abogado, a promover la presente acción de habeas data contra la Policía Nacional, explicando que habiendo su parte solicitado la expedición de un certificado de antecedentes penales en el mes de setiembre de 2001, la institución encargada le expidió

una constancia en la cual su parte registraba antecedentes por los hechos de abigeato, robo, asalto, posesión y tenencia de marihuana. Sigue manifestando que al ser erróneos los datos consignados en la referida constancia, su parte remitió una nota al Comisario Principal DAEP V. V. Z., solicitándole la rectificación de estos datos. Señala que los datos consignados en el certificado de antecedentes serían de otra persona con el mismo nombre pero que no cuenta con cédula de identidad. Sostiene que luego de la presentación de la nota mencionada más arriba, la información obrante en el certificado expedido por la Policía Nacional fue rectificada, sin embargo, alega que en fecha 09 de junio de 2005 le fue expedido un nuevo certificado de antecedente policiales, en el cual nuevamente se consignó los antecedentes de su homónimo, y es ese motivo lo que lo lleva a plantear la presente acción a fin de que los datos obrantes en los registros de la Policía Nacional sean rectificados, por no corresponder a su persona sino a un homónimo.-

Por su parte, la Policía Nacional contesta la acción por medio de su presentante convencional, señalando que tal como lo manifiesta el recurrente, existiría otra persona con el mismo nombre que el actor, quien no contaría con cédula de identidad, razón por la cual sus antecedentes son cargados en el prontuario del actor. Solicita al Juzgado que antes de dictar sentencia, se corrobore la existencia del homónimo.- - - - - - - - - - - - -

La pretensión de la parte actora debe ser estudiada a luz del art. 135 de la Constitución Nacional el cual reza: “Toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos”, así también deben considerarse las leyes reglamentarias Nº 1682/2001 y 1696/2002. Las normas citadas son bastante claras para resolver la presente causa. Efectivamente, con las instrumentales presentada en autos se constata claramente que el presente es un típico caso de homonimia. Así, con el certificado del acta de nacimiento

presentado a fs. 05 de autos y la cédula de identidad obrante a fs. 02 de autos, ha quedado acreditado que el actor de esta demanda, el señor F. F. C., con cédula de identidad Nº 2286820, nació el 02 de abril de 1959 en la ciudad de Coronel Bogado, y es hijo del señor F. F. y T. C., en cambio, la persona que fuera condenada por la comisión de los delitos consignados en el certificado de antecedentes presentado por el actor a fs. 08 de autos, es el señor F. F. C., que no constan que posea cédula de identidad, nacido en la ciudad de Belén, departamento de Concepción, en fecha 03 de diciembre de 1954, hijo de M. F. y F. C., lo que se acredita con la copia autenticada de la S.D. Nº 06 de fecha 03 de junio de 1998, dictada por el Juzgado de Primera Instancia en lo Criminal y Correccional del menor del Segundo Turno, de la Circunscripción Judicial de Pedro Juan Caballero y la copia del prontuario de mismo, remitido por el Director de la Penitenciaría Regional de Pedro Juan Caballero, lugar en que éste compurgó la condena que le fuera impuesta. Es dable destacar que la misma parte demandada admite que en el pasado ya se cometió el error de cargar los antecedentes penales del homónimo en el prontuario del actor de esta acción, situación que fue subsanada mediante la nota presentada por éste a la institución demandada (fs. 09), lo que apoya aún más la posición del actor. En estas condiciones, el Juzgado concluye que corresponde hacer lugar a la presente acción de Habeas Data, en consecuencia, deberá oficiarse al Departamento de Identificaciones a fin de que rectifique los datos del actor y se abstenga de consignar en el prontuario del mismo los datos o antecedentes judiciales de cualquier otra persona que no sea el actor.-

En cuanto a las costas, siendo que la demandada en ningún momento se opuso a la rectificación de los datos del accionante, sino que simplemente solicitó la corroboración fehaciente de la existencia de un homónimo para así luego subsanar el error cometido, lo cual es perfectamente entendible y razonable para el Juzgado, corresponde imponerlas en orden causado.-

Por lo tanto, el Juzgado-

R E S U E L V E:

1) HACER LUGAR a la presente acción de Habeas Data promovida por F. F. C., con cédula de identidad No 2286820, contra la POLICIA NACIONAL (DEPARTAMENTO DE IDENTIFICACIONES), y en consecuencia, ORDENAR a la demandada a que proceda a la inmediata rectificación de los datos del actor que obren en sus registros y se abstenga de consignar en el prontuario del mismo los datos o antecedentes judiciales de cualquier otra persona que no sea el actor. LIBRAR el correspondiente oficio

2) IMPONER las costas en el orden causado.-

3) ANOTAR, registrar y remitir copia a la Excma. Corte Suprema de Justicia.-

Firmado: Alma Mendez de Boungermini, Jueza.
Ante mí: Arnaldo Alvarez, Actuario.

JUICIO: "O. R. L. G. c/COLEGIO MARÍA AUXILIADORA S/ HABEAS DATA".-

ACUERDO Y SENTENCIA NÚMERO: SIETE

Asunción, 27 de febrero de 2007

VISTO: el presente juicio del que-

R E S U L T A:

Que en fecha 14 de diciembre de 2006 se presentó el Abogado H. S. A. en representación de la señora O. R. L. G., a promover acción de habeas data contra el COLEGIO MARÍA AUXILIADORA, en el escrito de fs. 14 de autos, manifestando entre otros puntos: "… mi mandante fuera docente en el Colegio María Auxiliadora de esta Capital de donde fue despedida por existir supuestamente una denuncia formulada por la Sra. R. A., abuela de un alumno … Que, los directivos de la Institución de enseñanza se han negado a proporcionarla los datos y el contenido de la denuncia que fuera formulada por la Sra. R. A., y redactada en el libro de actas por la psicóloga del del Colegio la Sra. I. M. de R., en el mes de octubre del corriente año y como testigo tengo al Escribano C. G. H. S., a quien le manifiesto que existe una denuncia en su contra en oportunidad de ir a realizar un Acta Notarial en la Dirección del Colegio …

Que, requerida la Directora de Nivel Sor M. C. B. G., el motivo de su despido, le manifestó que es por la denuncia realizada en su contra por la Abuela de uno de los alumnos, pero negándose a exhibirla el acta o explicarla el contenido de la misma, razón por la cual se plantea esta acción, en salvaguarda de su buen nombre y reputación…".-

Que por providencia de fecha 14 de diciembre de 2006, se tuvo por reconocida la personería del recurrente en el carácter invocado, por constituido su domicilio en el lugar señalado, y por iniciada la presente acción de habeas data que promueve la señora O. R. L. G. contra el Colegio María Auxiliadora y de la misma y de los

documentos acompañados se corrió traslado a la adversa por todo el término de ley.-

Que en fecha 28 de diciembre de 2006 se presentó el abogado R. A. P. F. en presentación del CENTRO EDUCATIVO MARÍA AUXILIADORA, a contestar la demanda en el escrito de fs. 65/73 de autos, manifestando entre otros puntos: "… Que no es verdad que los Directivos de la Institución. El Colegio María Auxiliadora, se haya negado a exhibir y/o proporcionar datos sobre una supuesta denuncia en contra de la Profesora Señora O. R. L. G… Que, como SS., podrá apreciar la institución educativa "El Colegio María Auxiliadora", cuenta con un plantel de profesores que son seleccionados cada año atendiendo a su calidad profesional, y como requisito el título que lo habilite como tal … Dentro del programa académico de la institución se realiza la selección de maestros, tarea a la cual la institución se aboca cada año, para lo cual se observan varios criterios atendiendo al desempeño que ha tenido un profesor, la receptividad de sus enseñanzas en los alumnos, su grado de responsabilidad, y la vocación con la cual se ha desempeñado durante el año lectivo … No obstante siendo una institución privada abocada a una misión de suma importancia como lo es, reitero, la formación de niños y jóvenes, se acuerda la redacción de un contrato de trabajo, cuya duración es la de UN AÑO LECTIVO … Luego, se procede a una revisión como ya lo señalara de todos los objetivos que han sido cumplidos durante el año y un análisis de aquellos que no han podido de alguna u otra forma alcanzarse …Ahora bien, la Profesora O. R. L. G., ha firmado con la institución un Contrato individual de trabajo por el año lectivo correspondiente al 2006 …al finalizar el año, la institución ha optado como resulta de su legítimo derecho, rescindir el contrato, darlo por terminado …Es absolutamente falsa su apreciación de que por motivos de una denuncia se haya optado a su despido …Lo cierto es que como es normal, siempre existen quejas de algunos padres, como los hay y los habrá siempre, dada la cantidad de niños y jóvenes que acuden a diario a la institución de mi mandante, pero, que se hubiese tomado la decisión de prescindir de sus servicios se debe a una decisión de orden estrictamente académica, y no con la intención de manchar el nombre y/o reputación de la profesora O. R. L. G. …No existe

ninguna denuncia redactada en acta, pues no resulta de nuestra función hacerla, sí recibimos a los padres o encargados cuando estos quieran comunicarnos alguna cuestión con respecto a sus hijos, o nosotros optamos por llamarlos cuando alguna cuestión así lo amerite …Es por ello que sostenemos que la acción de habeas data no puede prosperar cuando que no existe una información que proporcione un descrédito o una falsa información que dañe a la persona de la accionante …NO se ha probado la existencia de una falsedad en la información o el error en el contenido de los documentos que se acompañan, y de los mismos no puede inferirse en un daño ilegítimo por tanto la acción de habeas data debe ser rechazada con expresa condena en costas…".-

Que por proveído el 21 de febrero de 2007, el Juzgado reconoció la personería del recurrente en el carácter invocado, por constituido su domicilio en el lugar señalado, y no existiendo pruebas que diligenciar se llamó AUTOS PARA SENTENCIA.-

C O N S I D E R A N D O:

Que la actora O.R.L.G. inicia acción de habeas data contra el COLEGIO MARÍA AUXILIADORA; explica que se desempañaba en dicha institución como docente y que fue despedida por una supuesta denuncia que habría formulado una persona de nombre Rosa Almirón, abuela de uno de sus alumnos. Sigue señalando que los directivos de la institución se han negado en todo momento a proporcionarle una copia de la mentada denuncia, por lo que promueve la presente acción a fin de que le sea proporcionada una copia de la mencionada denuncia.-

Por su parte la demandada CENTRO EDUCATIVO MARÍA AUXILIADORA contesta la acción por medio de su representante convencional, señalando que si bien es cierto la actora fue despedida de la institución, ello no fue producto de denuncia alguna. Señala que en la institución no obra ningún tipo de denuncia contra la accionante, y que no es competencia de los directivos del colegio labrar acta de las quejas formuladas por los padres de los alumnos. Sigue manifestando que si bien es cierto siempre existen quejas o requerimientos de los padres, ninguna de

ellas fue la causante del despido de la accionante, lo cual se debió a que ésta simplemente no reunía los requisitos exigidos por los directivos de la institución.-

La pretensión de la parte actora debe ser estudiada a la luz del art. 135 de la Constitución Nacional el cual reza: "Toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos". La norma citada es bastante clara, en efecto, en el caso de autos la accionante alega que existe un acta en la cual se dejó constancia de una supuesta denuncia que habría realizado la abuela de uno de los alumnos de la institución, sin embargo, este hecho fue negado rotundamente por la parte demandada. En ese sentido, a la parte actora le correspondía acreditar sus argumentos con las pruebas idóneas para el efecto, sin embargo no lo hizo así. Efectivamente, la accionante pretende probar la existencia de una supuesta denuncia en su contra en la institución demandada, con la copia del acta notarial labrada en fecha 28 de noviembre de 2006 en el Colegio María Auxiliadora a pedido de su parte (fs. 11/14), sin embargo de la misma no surge que se haya labrado acta alguna con referencia a una supuesta denuncia. En efecto, si bien es cierto la representante de la institución educativa que recibió al Escribano Público, Sor M. C. B. G. dio a entender que los padres de un alumno habrían formulado una queja en contra de la accionante, no es menos cierto que también sostuvo que esta no le había mencionado nada al respecto y que ese tema lo venía tratando con la Directora General de la Institución, Sor T. de J. P. En este punto debe realizarse algunas precisiones; en primer lugar la señora M. C. B. G. en ningún momento manifestó que se haya labrado acta de una supuesta denuncia formulada por los padres de un alumno. En segundo lugar en su escrito de demanda la actora sostuvo que la denuncia de la que se habría dejado constancia en acta la había realizado la abuela de un alumno, en cambio en el acta notarial mencionada más arriba alegó que la queja habría provenido de los padres de un estudiante. Debido a lo señalado precedentemente el Juzgado

concluye que las pruebas arrimadas a autos por la actora, no acreditan fehacientemente el hecho generador de la presente acción, es decir, la supuesta denuncia que se habría dejado constancia en acta, ya que la demandada si bien admitió que en ocasiones los padres de los estudiantes de la institución presentan quejas o requerimientos, negó que se haya dejado constancia de los mismos. Por otra parte las, demás instrumentales arrimadas con la demanda no guardan relación con el hecho expresado en el escrito de demanda por la trabajadora, por lo que nada aportan para la resolución de la causa. En estas condiciones, al no haber demostrado la actora la existencia del documento motivador de la presente acción de habeas data y no existiendo obligación legal por parte de la demandada de contar con dicha instrumental, corresponde rechazar la presente acción.-

POR TANTO, de conformidad a las disposiciones legales citadas en Juzgado: -

R E S U E L V E:

1) NO HACER LUGAR a la acción de Habeas Data promovida por O. R. L. G. contra CENTRO EDUCATIVO MARÍA AUXILIADORA, por los fundamentos expuesto en el considerando de la presente resolución.-

2) IMPONAR las costas a la parte actora.-

3) ANOTAR, registrar y remitir copia a la Excma. Corte Suprema de Justicia.-

Firmado: Alma Mendez de Boungermini, Jueza.
Ante mí: María de la Cruz Rodríguez, Actuaria Judicial.

JUICIO: C.A.R. c/ INFORMCONF (INFORMES CONFIDENCIALES) s/ INDEMNIZACIÓN DE DAÑOS Y PERJUICIOS. AÑO: 2000. Nº 7. FOLIO 32. SECRETARÍA Nº 8.-

S.D. Nº 416

Asunción, 2 de agosto de 2007.-

VISTO: El presente juicio, del que; -

RESULTA:

QUE, en fecha 4 de agosto de 2000, se presentó ante el Juzgado de igual clase y jurisdicción del Tercer Turno, el abogado CAR, en causa propia y bajo patrocinio de la abogada MRB, a promover juicio de indemnización de daños y perjuicios contra la firma INFORMCONF (INFORMES CONFIDENCIALES), manifestando que sufrió, a causa de haber la demandada, emitido informes confidenciales sobre su situación patrimonial, que se ajustaron "a la realidad y a la verdadera situación actualizada" del mismo. Explica que, a pesar de haber cancelado sus respectivas deudas con los Bancos de Desarrollo y Unión, la empresa accionada siguió emitiendo informes como si fueran todavía y, a pesar de ello, operaciones morosas. Tales informes, carentes de veracidad, continuaron en la base de datos de la demandada. El monto reclamado en el presente juicio, en concepto de indemnización, comprende: 1.-DAÑO MORAL: Gs. 150.000.000. 2.-DAÑO EMERGENTE: Gs. 19.000.000. 3.-LUCRO CESANTE: Gs. 31.000.000; TOTAL: Gs. 200.000.000 (fs. 187/198).-

QUE, por proveído de fecha 21 de noviembre de 2000 (fs. 199), el Juzgado de Primera Instancia en lo Civil y Comercial del Tercer Turno, tuvo por iniciado el presente juicio por indemnización de daños y perjuicios, y dispuso que se corra traslado de la demanda a la parte demandada para que la conteste dentro del plazo de Ley.-

QUE, en fecha 19 de marzo de 2000 (fs. 218/234), se presentó el abogado JCF, en nombre y representación de la firma INFORMCONF S.A., bajo patrocinio del abogado AR, a recusar sin

expresión de causa al Juzgado citado y a contestar la demanda incoada, manifestando que el demandante no probó los hechos configurativos de los daños, tanto los materiales como el moral reclamados; controvirtiendo, además, el derecho invocado por el peticionante de la reparación indemnizatoria, sosteniendo que éste no ha demostrado dedicarse a la actividad comercial. Sostiene que, en el caso, ni INFORMCONF ni sus Directores han tenido mala fe, ni dolo y "que su accionar ha sido claro y transparente, no ha habido una conducta punible". Negó, igualmente, que el actor haya experimentado los daños patrimoniales que reclamó en su demanda.-

QUE, por providencia de fecha 23 de mayo de 2001 (fs. 235), el Juzgado de igual clase y jurisdicción del Tercer Turno se separó de seguir entendiendo en estos autos, remitiendo los mismos a este Juzgado.-

QUE, por proveído de fecha 4 de abril de 2001 (fs. 235 vlto.), este Juzgado dictó el proveído de tener por recibidos estos autos y que se haga saber el mismo a las partes.-

QUE, en fecha 20 de setiembre de 2001 (fs. 238/241), se presentó el representante convencional de la parte demandada a solicitar caducidad de instancia.-

QUE, por A.I. Nº 1698 de fecha 2 de octubre de 2003 (fs. 251), el Juzgado resolvió no hacer lugar a la caducidad de instancia solicitada por la parte demandada.-

QUE, por providencia de fecha 16 de marzo de 2004 (fs. 249), el Juzgado, atento al escrito obrante a fs. 218/234, a mérito del testimonio de Poder General presentado, reconoció la personería del recurrente en el carácter invocado y por constituido su domicilio en el lugar indicado. De la contestación de la presente demanda se solicitó que, previamente, se agregue la cédula de notificación del proveído de fecha 27.11.2000.-

QUE, por proveído de fecha 16 de abril de 2004 (fs. 252), el Juzgado, habiéndose dado cumplimiento al proveído de fecha

16.03.2004, a mérito del testimonio de Poder General presentado, reconoció la personería del recurrente en el carácter invocado y por constituido su domicilio en el lugar indicado. Ordenó el desglose y devolución de los documentos originales presentados, previa autenticación de sus fotocopias por la Actuaria. Tuvo por contestado el traslado de la presente demanda y de los documentos presentados corrió traslado a la parte actora por todo el plazo de ley, quien lo contestó en los términos del escrito de fs. 253/254.-

QUE, por proveído de fecha 6 de octubre de 2004 (fs. 254 vlto.), el Juzgado se consideró competente para entender en la presente litis y, existiendo hechos controvertidos que probar, ordenó la apertura de la causa a prueba por todo el plazo de ley.-

QUE, por proveído de fecha 28 de abril de 2005 (fs. 376), atento al informe de la Actuaria, el Juzgado ordenó el cierre del período probatorio, dispuso la agregación de las instrumentales presentadas y que, una vez firme el citado proveído, se pasen estos autos a las partes por su orden para que presenten sus correspondientes escritos de alegatos en el plazo de seis días.-

QUE, por providencia del 16 de mayo de 2005 (fs. 386 vlto.), se ordenó la agregación del escrito de alegatos de la parte actora, como asimismo, por providencia de esa misma fecha, (fs. 391), se ordenó la agregación del escrito de alegatos, correspondiente a la parte demandada y, en consecuencia, se llamó autos para sentencia, y;-

CONSIDERANDO:

El Abogado C. A. R. A. demanda en autos (fs. 187/198) a la empresa INFORMCONF S.A. por indemnización de los daños y perjuicios que dice sufrió a causa de haber la demandad emitido informes confidenciales sobre situación patrimonial, que no se ajustaron "*…a la realidad y a al verdadera situación actualizada…"* del mismo. Explica que, a pesar de haber cancelado sus respectivas deudas con los Bancos de Desarrollo y Unión, la empresa accionada siguió emitiendo informes como si fueran todavía y, a pesar de ello, operaciones morosas. Tales informes, carentes de

veracidad, continuaron en la base de datos de la demandada, no obstante la nota que le fuera cursada por el Abogado R., en fecha 21 de julio de 1.998 (fs. 10). El recibo, sin embargo de esta comunicación, fue expresamente negado por la accionada en su contestación. Al respecto, es necesario advertir que al pie de esta nota existe constancia que dice, textualmente: *"Recibido 21 jul 1998. Existe una firma. 1053 hs. S. S."*. Nótese, que esta leyenda carece de todo elemento que permita identificarla como expedida por la empresa destinataria, por lo que no se trata – en el caso – del supuesto previsto en el Art. 307 del Código Procesal Civil.-

La empresa accionada contestó el traslado de la demanda a fs. 218/234, oponiéndose en general, y también puntualmente, a las pretensiones del actor. Dijo – entre otras cosas – que el demandante o probó los hechos configurativos de los daños, tanto los materiales como el moral, reclamados; controvirtiendo, además, el derecho invocado por el peticionante de la reparación indemnizatoria, sosteniendo que éste o ha demostrado dedicarse a la actividad comercial. Sostiene –asimismo- que, en el caso, ni INFORMCONF ni sus directores han tenido mala fe ni dolo, y *"…que su accionar ha sido claro y transparente, no ha habido una conducta punible.."*. Negó, igualmente, que el actor haya experimentado los daños patrimoniales que reclamó en su demanda.-

Sobre el tema, al tiempo de expedirse el informe cuestionado, vale decir el 31 de enero del año 2000, no se encontraban aún vigentes las leyes 1682/2001 y 1969/2002, reglamentarias de las informaciones de carácter privado.-

Pero –no obstante ello- cuando un hecho no transgredí un deber jurídico concreto o determinado, nacido del contrato o convención, de la voluntad unilateral, del desplazamiento patrimonial incausado o impuesto por la ley, etc., sino que viola el deber genérico de no dañar a las personas en sí mismas o en sus bienes (*naeminem laedere),*estamos frente a un hecho ilícito (Gabriel A. Stiglitz y Carlos A. Echevesti, Daño Moral, en colección de Responsabilidad Civil, Ed. Hammurabi, dirigida por Jorge Mosset Iturraspe, p. 249).-

El Art. 26 de la Constitución Nacional, prescriba: "…Toda persona tiene derecho a generar, procesar o difundir información, como igualmente a la utilización de cualquier instrumento lícito y apto para tales fines". Y el art. 28 de la misma C.N. agrega: "Se reconoce el derecho de las personas a recibir información veraz, responsable y ecuánime. Las fuentes públicas de información son libres para todos. La ley regulará las modalidades, plazos y sanciones correspondientes a las mismas, a fin de que este derecho sea efectivo. Toda persona afectada por la difusión de una información falsa, distorsionada o ambigua tiene derecho a exigir su rectificación o su aclaración por el mismo medio y en las mismas condiciones que haya sido divulgada, sin perjuicio de los demás derechos compensatorios". El art. 33 de la Carta Magna, preceptúa: "La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, estará exenta de la autoridad pública. Se garantiza el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas".-

Atendiendo al precedente marco legal, de rango constitucional, encontramos que ha sido francamente antijurídica la conducta de la empresa demandada al no mantener invariable y permanentemente actualizada su base de datos con relación a la situación patrimonial y crediticia del Abg. C. A. R. A., suministrando –a causa de ello- informaciones inexactas sobre dicha persona, conforme ocurrió con las obligaciones adeudadas a los Bancos de Desarrollo Unión, que figuraron como morosas o pendientes de pago en el formulario expedido por la firma INFORMCONF, en fecha 31 de enero de 2000 (fs. 08/09), documentos estos que fueron reconocidos como válidos en la absolución de posiciones de la demandada de fs. 291, cuando en ese tiempo ya se encontraban satisfechas y canceladas, según se interfiere de los términos de la contestación a la demanda de autos.-

La antijuridicidad de ese comportamiento de la empresa demandada no encuentra justificación legítima, aunque fuera cierto que esas cancelaciones no le hubieran sido comunicadas por el interesado o por los acreedores, dado el deber que tiene toda

persona física o jurídica, de conducirse con atención y diligencia para no causar daños a otros, conforme con la definición legal de la culpa, explicitada en el norma del art. 421 del Código Civil: *"Habrá culpa cuando se omitieren aquellas diligencias exigidas por la naturaleza de la obligación y que correspondan a las circunstancias de las personas, tiempo y lugar…".-*

Al respecto de lo apuntado en el párrafo anterior, es conveniente destacar que el dato sobre el hecho de haber sido demandado el Abogado R. por una deuda pendiente que mantenía con el Banco de Desarrollo, fue obtenido por INFORMCONF recurriendo a las fuentes públicas de información conforme con la facultad reconocida en el art. 28 de la Constitución Nacional. Siendo así, no se explica razonablemente que de obrar con diligente eficiencia – como era su deber, y es el de todos, genéricamente hablando – no utilizara el mismo mecanismo para recoger el hecho de haberse finiquitado el aludido proceso ejecutivo de cobro judicial. Recuérdese que la misma norma constitucional, empieza diciendo que todas las personas tienen el derecho de recibir información *veraz y responsable* (art. 28 C.N.).-

Así entonces, sobre dicha circunstancia puntual, la información brindada por la empresa demandada, no ha sido – por cierto – ni veraz ni tampoco responsable. Y, repetimos a este propósito que no hay excusa válida que explique el comportamiento, verdaderamente displicente, de la firma que comercializa informes sobre la situación patrimonial de los ciudadanos. Pues, es lógico suponer y esperar, que se conduzca – desde luego – con la misma presteza y diligencia que tuvo cuando recaudó los respectivos datos de la morosidad. Su deber de comportarse con eficiencia, y de ser veraz, no dependen ni están condicionados por actividad alguna del afectado; por ejemplo, de una comunicación del mismo.-

Otro tanto debe decirse con relación al argumento de la empresa demandada sobre la existencia de contratos celebrados entre ella y los bancos, financieras y otras instituciones de crédito, por los que estos últimos asumieron el compromiso de comunicar a INFORMCONF sobre las cancelaciones de las deudas morosas,

pues se tratan – obviamente – de convenios que – en virtud del principio del efecto relativo de los actos jurídicos (artículo 717 del Código Civil) – sólo producen consecuencias entre las partes del mismo, siendo – por ello mismo – inoponibles ni invocables respecto de terceros. En nuestro caso, pues, tales convenciones no extendían sus consecuencias a un tercero, tal lo era el Abogado C. A. R. (véanse los ejemplares de estos contratos agregados a fs. 209 y 214).-

Teniendo, entonces, en consideración las normas transcriptas de la Constitución Nacional, debemos expresar que media en el caso, como perfectamente constatado, otro de los elementos esenciales de la indemnización de daños, vale decir, el de la antijuridicidad o ilicitud, conforme se lo exige en el art. 1834, inc. a) del Código Civil.-

El hecho de que el Abogado R. tuviera otras demandas ejecutivas, u obligaciones morosas, no justifica la conducta omisiva y desatenta de la empresa demandada, que comercializa el rubro de los informes sobre estados patrimoniales y ello, por el deber genérico ya señalado, de no dañar a otros *(neminem laedere)*.-

En lo que se refiere a los daños materiales que dice haber sufrido el actor, debemos señalar que los mismos no han sido correctamente definidos en la demanda, ni han sido tampoco objeto de acreditamiento adecuado. En efecto, la circunstancia de que se le haya rehusado algunas tarjetas de crédito, por sí sola, no prueba la existencia de daño. Ello es así, porque se tratan de operaciones financieras concebidas para el consumo de sus usuarios y, a éstos –en principio- no le producen beneficios lucrativos. Las adquisiciones pagadas con la tarjeta de crédito, constituyen deudas de dinero que deben ser devueltas a las empresas emisoras, con intereses. Para estos últimos, la explotación del negocio de las tarjetas de crédito les representa efectivamente, utilidades financieras.-

Ante esa realidad conceptual, era deber del demandante demostrar los daños materiales concretos que experimentó por

motivo de habérsele negado las tarjetas de crédito. No lo ha hecho así, por lo que su reclamo en tal sentido no puede prosperar.-

En cuanto al lucro cesante, tampoco dicho rubro ha sido acreditado debidamente, al no haberse justificado cual es el beneficio o ganancia que ha dejado de percibir como consecuencia del acto ilícito.-

No ocurre lo mismo con respecto al daño moral, pues la negligencia de la demandada es realmente inexcusable. En efecto, la parte accionada no argumentó ningún motivo de caso fortuito o fuerza mayor, o el hecho de un tercero por quien no deba responder (arts. 422 y 426 del Código Civil), que pudieran exonerarle de las consecuencias de su acto ilícito, según se consagra en la norma de los arts. 1833 y 1834 inc. c) del mismo cuerpo legal.-

Sobre el particular establece el art. 451 del Código Civil: "Cuando la obligación no cumplida proviniere de actos a título oneroso, y en todos los demás casos en que la ley lo autorice, habrá lugar a resarcimiento, aunque el perjuicio no fuera patrimonial, debiendo el juez estimar su importe con arreglo a las circunstancias".-

Para determinar la existencia del daño moral reclamado, resulta necesario asumir lo que ocurre en la realidad de la vida, en las relaciones de los miembros de una comunidad y, muy especialmente en la índole de los comportamientos habituales de los seres humanos quienes, expuestos a una situación semejante, de una ofensa injusta a su dignidad, experimentan, en casi todos los casos, el dolor propio de las lesiones que vulneran el espíritu. Lo contrario, es excepcional, pues son escasas las personas que permanecen inalteradas en tales circunstancias. En el caso, resulta indudable la existencia de daño moral en detrimento personal del demandante, por causa del relatado comportamiento injusto de la empresa demandada.-

La prueba de la existencia del daño moral, en el caso de autos, surge nítida de lo expuesto en el párrafo anterior, pues "Para probar

el daño material basta aportar los elementos probatorios que lleven a la conciencia del Juez el convencimiento de la existencia de circunstancias objetivamente reveladoras de la presencia del perjuicio y su entidad. Para probar el daño moral en su existencia y entidad no es necesario aportar prueba directa, sino que el Juez deberá apreciar las circunstancias del hecho y las calidades morales de la víctima para establecer objetiva y presuntivamente el agravio moral en la órbita reservada de la intimidad del sujeto pasivo. No creemos que el agravio moral debe ser objeto de prueba directa pues ello resulta absolutamente imposible por la índole del mismo que reside en lo más íntimo de la personalidad…" (Jorge Bustamante Alsina, Equitativa valuación del daño no mensurable, La Ley 1990-A, 654).-

Podemos definir entonces el daño moral como la lesión en los sentimientos que determina dolor o sufrimientos físicos, inquietud espiritual, o agravio a las afecciones legítimas y en general toda clase de padecimientos insusceptibles de apreciación pecuniaria (Jorge Bustamante Alsina, Teoría General de la Responsabilidad Civil, p. 179).-

Es también aplicable para la determinación del daño moral, la norma del artículo 1835 del Código Civil: "Existirá daño, siempre que se causare a otro algún perjuicio en su personal, en sus derechos o facultades, o en las cosas de su dominio o posesión. La obligación de reparar se extiende a toda lesión material o moral causada por el acto ilícito. La acción por indemnización del daño moral sólo competerá al damnificado directo. Si del hecho hubiere resultado su muerte. Únicamente tendrán acción los herederos forzosos".-

Teniendo en cuenta, además, que la reparación del daño moral tiene carácter resarcitorio, y debe –consecuentemente- ser traducido en una condena de dinero, pues consideramos que *"Es cierto que el agravio moral se sustrae a una medición exacta y consecuentemente a una traducción dineraria, no obstante, debe tenerse en claro que al intentar componerlo el derecho no busca una equivalencia. El daño moral, no se borra ni desaparece por la suma de dinero que se conceda a la víctima: la finalidad perseguida no es*

sino la de permitirle al perjudicado alguna suerte de satisfacción para mitigar el estado; el dinero es, por el momento, el único medio conocido para que la víctima pueda sobrellevar mejor el dolor injustamente padecido, procurándose satisfacciones sustitutivas" (Gabriel A. Stiglitz y Carlos A. Echevesti, Daño Moral, op. cit. P. 246).-

Prestando pues atención al marco legal y doctrinal señalado, el Juzgado considera que la empresa demandada debe ser condenada a resarcir al actor, el daño moral que le causó su conducta relacionada más arriba, abonándole la suma de GUARANÍES NOVENTA MILLONES (Gs. 90.000.000), en tal concepto.-

En cuanto a las costas, las mismas deben ser impuestas a la perdidosa, conforme al principio general establecido en el art. 192 del Código Procesal Civil.-

POR TANTO, atenta a las consideraciones que preceden, y a las disposiciones legales citadas, el Juzgado de Primera Instancia en lo Civil y Comercial del Cuarto Turno.-

R E S U E L V E:

1) HACER LUGAR, con costas, a la demanda de indemnización de daños y perjuicios promovida en auto s por el Abg. C. A. R. A., en contra de la empresa INFORMCONF SOCIEDAD ANÒNIMA, y condenar en consecuencia a esta última a pagar al actor la suma de GUARANÍES NOVENTA MILLONES (Gs. 90.000.000) en el plazo de cinco días de hallarse firme esta resolución, en concepto de indemnización del daño moral causándole.-

2) ANOTAR, registrar y remitir copia a la Excma. Corte Suprema de Justicia.-

Firmado: Judith Gauto Bozzano, Jueza.
Ante mi: Martha Torres, Secretaria.

JUICIO: "N. M. V. C. F. de L. c/ POLICIA NACIONAL, DEPARTAMENTO DE IDENTIFICACIONES s/ HABEAS DATA".-

S.D. N^{O} 86

Asunción, 09 de julio de 2008.-

VISTO: La presente acción de Habeas Data de la que-

R E S U L T A:

Que eh la fecha 13 de mayo de 2008, se presentó ante este Juzgado la señora N. M. V. C. F. de L., por derecho propio y bajo patrocinio de abogado, a promover juicio de hábeas data manifestando cuanto sigue: "…Que recurro ante el órgano jurisdiccional a *peticionar la rectificación o destrucción de los datos que obran en la Policía Nacional Sección Estadísticas* teniendo en consideración que dichos datos afectan ilegítimamente mis derechos de la siguiente manera: Que la referida institución ha procedido a registrar mi nombre en su base de datos por una Causa Judicial caratulada N. M. V. C. F. de L. s/ LESIÓN DE CONFIANZA y OTROS habiendo a la fecha cumplido con la sanción que me ha impuesto el Juzgado interviniente con el pago de la multa conforme lo justifico con los documentos que acompaño. Que sumado a eso es preciso poner a conocimiento de esta Magistratura que los querellantes han desistido de la acción tanto civil y penal contra mi persona conforme al Acta Notarial N^{o} 19 de fecha 13 de mayo de 2002 expedida ante la Escribana Pública M.I.B.O.; en donde se estipula que dicho instrumento servirá como suficiente prueba de dicho desistimiento ante las autoridades s instituciones pertinentes… Que los datos e informaciones aun obrantes en mi prontuario Policial, en la base de datos proporcionados por la Policía Nacional, no me permiten una reinserción total y absoluta como lo contempla nuestra Constitución Nacional, el Pacto de San José de costa Rica y la Ley Penal; ya que la información proporcionada por la Policía Nacional (Certificado de Buena Conducta), atenta ilegítimamente contra el derecho a la imagen de mi persona, más aun cuando pretendo ejercer la profesión de Abogado, con la presentación de mis antecedentes para concursar

para una función judicial o fiscal, o ser parte de una Estudio Jurídico, impidiendo de esta forma el libre ejercicio e la profesión y el derecho a un trabajo digno, al ser marginada sistemáticamente por dicho motivo, considerando que por sus errores ya cumplió con la Sociedad, continúa siendo considerando por una Entidad Pública o Privada un ciudadano marginal sin derecho alguno, razón por la cual permito SEÑALAR a V.S., que la información señalada afectan mis derechos… Que además al haber los querellantes desistido de las acciones contra mi persona y cumplido con la sanción que me fuera aplicada por el Juzgado interviniente, corresponde que la Policía Nación excluya dichos datos obrantes en mí prontuario, en el momento de expedir la constancia DEL CERTIFICADO DE BUENA CONDUCTA, que afectan ilegítimamente a los derechos a mi imagen pública, intimidad, el libre ejercicio de mi personalidad, a un trabajo digno, a la protección de la familia y de los hijos, por sobre todo los Derechos Humanos fundamentales, consagrados en la Constitución Nacional, en loa Convenios Internacionales ratificados y canjeados por nuestro país, vigentes por el art. 137 CN… que, la garantía constitucional del HABEAS DATA tiende a garantizar al individuo su libertad, igualdad y veracidad en relación a los demás ciudadanos siendo que a través de las informaciones obrantes en prontuarios o archivos se pueden ocasionar innumerables perjuicios a la persona que atentan contra sus derechos personalísimos..". Termina solicitando que, oportunamente se dicte sentencia haciendo lugar a la acción del habeas data, ordenando la destrucción, modificación o exclusión de datos registrados sobre su persona en la Policía Nacional.-

Que el Juzgado por providencia de fecha 16 de mayo de 2008, tuvo por presentada a la recurrentes en el carácter invocado, por constituido su domicilio en el y por iniciada la demanda de habeas data, asimismo se corrió traslado de la misma a la parte demandada por todo el término de ley. Por A.I. N° 330 de fecha 07 de julio de 2007se acusó de rebeldía a la Policía Nacional – Departamento de Identificaciones y se dio por decaído el derecho que tenia para contestar el traslado que se le corriera por providencia de fecha 16 de mayo de 2008, en consecuencia se llamó Autos para Sentencia.-

C O N S I D E R A N D O:

La actora N. M. V. C. F. de L., por derecho propio y bajo patrocinio de abogado, inicia la presente acción de Habeas Data solicitando al Juzgado que ordene a la Policía Nacional la exclusión de los datos registrados sobre su persona en esa repartición pública. Explica que la Policía Nacional registra en su base de datos una causa judicial caratulada "N. M. V. C. F. de L. s/LESIÓN DE CONFIANZA y OTROS", agrega que sin embargo, los querellantes han desistido de la acción tanto civil como penal contra su persona conforme al acta notarial que adjunta y que ha cumplido con la sanción aplicada por el Juzgado. Argumenta que la información proporcionada sobre su persona por la demandada a través del certificado de buena conducta, no le permiten una reinserción total y absoluta a la sociedad, agrega que atenta ilegítimamente contra su derecho a la imagen más aun cuando pretende ejercer la profesión de abogada, con la presentación de sus antecedentes para concursar por un cargo en la función judicial o fiscal o ser parte de un estudio jurídico, circunstancias estas que le impiden el libre ejercicio de la profesión y el derecho a un trabajo digno.-

La pretensión de la parte actora debe ser estudiada a la luz del art. 135 de la Constitución Nacional el cual reza: "Toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectarán ilegítimamente sus derechos", así también deben considerarse las leyes reglamentarias Nº 1682/2001 y 1696/2002. la norma constitucional citada más arriba faculta a la actora a solicitar la destrucción, la actualización y rectificación de los datos erróneos que existan sobre su persona o sobre sus bienes, sin embargo, de las constancias de autos surge que no existe ningún dato erróneo que deba ser rectificado, excluido o destruido. Efectivamente, si bien a la Policía Nacional se le declaró rebelde por no presentar al Juzgado el informe correspondiente, no puede desconocerse que la propia actora admite haber sido sujeto de una causa penal en la cual recayeran resoluciones judiciales, a la fecha

firmes y ejecutoriadas, en las cuales se califica de antijurídica la conducta de la misma (Acuerdo y Sentencia Nº 31 del 26 de abril de 2002 y S.D. Nº 18 del 08 de mayo de 2001 a fs. 07/15), inclusive la actora reconoce que la pena aplicada por el Juzgado ya la ha cumplido. En definitiva, la propia actora reconoce la veracidad de los datos proporcionados por la Policía Nacional sobre su persona a través del Certificado de Buena Conducta. Debe aclararse que en este caso la actora no alega que la institución demandada estuviera dando datos incompletos o incorrectos en cuanto a no especificar que la causa concluyó habiendo la misma cumplido la pena que se le impusiera, en cuyo caso el Juzgado podría ordenar la rectificación de los datos en cuestión. Lo que la actora pretende, es que el Juzgado ordene la exclusión de datos cuya veracidad admite. Si bien son comprensibles los argumentos esgrimidos en la demanda en cuanto a que la proporción de tales datos por parte de la Policía Nacional, podría acarrearle a la actora inconvenientes en su reinserción a la sociedad, sin embargo, tales argumentos ceden ante el bien jurídico protegido cual es la seguridad jurídica preventiva de la sociedad. Puestas así las cosas, esta Magistratura no puede disponer la destrucción, exclusión o borrado de los datos verdaderos que sobre la accionante obran en su prontuario policial, por lo que deberá rechazarse la presente acción de habeas data en base a las razones expuestas líneas más arriba.-

POR TANTO, de conformidad a las disposiciones legales citadas en el Juzgado.-

R E S U E L V E:

1) NO HACER LUGAR a la acción de Habeas Data promovida por N. M. V. C. F. de L. contra la POLCIA NACIONAL, conforme a lo explicado en el considerando e la presente resolución.-

2) ANOTAR, registrar y remitir copia a la Excma. Corte Suprema de Justicia.-

Firmado: Alma Mendez de Boungermini, Jueza.
Ante mí: Arnaldo Alvarez Figueredo, Actuario Judicial.

JUICIO: "HÁBEAS DATA SOLICITADO POR L. R. S. c/INFORMCONF S.A.".-

S.D.N^{O}: 29

VISTOS: Estos autos de los que.-

R E S U L T A:

Que, a fs. 3/6 de autos consta el escrito presentado por el Sr. L. R. S., bajo patrocinio del Abogado M. A. P., por el cual solicita la Garantía Constitucional del Hábeas Data.-

Que, a fs. 07 de autos, obra el proveído de fecha 30 de abril de 2009, y a fs. 08 el oficio pertinente remitido a la Firma INFORMCONF S.A. requiriendo la remisión de datos que obren en sus registros con relación a L. R. S., así como de la autorización correspondiente para la difusión y publicación de datos personales del demandante.-

Que, a fs. 9/16 de autos, obra el Poder Especial otorgado a favor del Abogado I. A. R. S., así como el informe y escrito presentado por la firma INFORMCONF S.A. a través de su representante legal y, .-

C O N S I D E R A N D O:

Que, en fecha 27 de abril de 2009, EL Señor L. R. S., a través de su patrocinante el Abogado M. A. P., plantea la Garantía Constitucional del Habeas Data, - según manifiesta – en los siguientes términos: "QUE, desde hace años la firma INFORMCONF, viene difundiendo información respecto a mi persona haciéndome aparecer como moroso, situación que me produce un gran daño no solo moral, sino también político y patrimonial que afecta mi buen nombre, honor y reputación como ciudadano paraguayo así también como en mis actividades comerciales, crediticias, financieras, sociales, laborales y políticas cotidianas. La inclusión de mi nombre en los "panfletos" de INFORMCONF" como demandado me impide acceder a créditos de

corto o largo plazos y también me perjudica en el ámbito político en el cual incursiono en la ciudad de Luque debido a que mis contendientes políticos se valen de dichos "panfletos" para desprestigiar mi buen nombre, honor y reputación jugando con mi dignidad de persona y hacer que pierda el crédito de mis adeptos y demás electores, lo que a su vez me produce un daño moral y social inescrutables ya que me impide acceder a eventuales cargos públicos y también a obtener prestamos en entidades comerciales o financieras..//…. Señoría, es cierto que demandado por cobro de guaraníes, ello no puede ser motivo para que en sus informes me hagan aparecer ante todos como paria ya que me estoy defendiendo y no existe aún sentencia firme y ejecutoriada que me haga aparecer como culpable,… terceras personas no pueden divulgar datos acerca de mis registros o de las operaciones comerciales que realicé con otras personas o entidades sino cuenta con alguna orden judicial, es el caso que la firma INFORMCONF no refiere tener orden judicial para brindar informes sobre mi persona y operaciones comerciales…//… el Sanatorio Migone, me negó el seguro médico debido a que mi nombre figura en los famosos informes de INFORMCONF, privándome así de recibir una atención médica calificada y oportuna por el consabido hecho de que los centros públicos están colapsados de pacientes… Por las razones expuestas y en atención a lo previsto en el art. 28 inc. 3 de la Constitución Nacional, impetro al Juzgado que aplicando estricta justicia, resuelva fundadamente y favorablemente a mí favor que la firma INFORMCONF se abstenga de en el futuro de seguir emitiendo en sus panfletos de que figuro en la lista de demandados, sin antes tener a la vista una resolución judicial que le permita informar sobre mí persona en dicho sentido".-

Que, por providencia de fecha 30 de abril de 2009, el Juzgado tuvo por presentado al recurrente, en el carácter invocado y por constituido su domicilio en el lugar indicado, asimismo, tuvo por iniciado este procedimiento de Hábeas Data promovido por el Sr. L. R. S. bajo patrocinio de Abogado en contra de la firma INFORMCONF, requiriéndose de dicha firma informes sobre los datos que obren en sus archivos con relación al Sr. L. R. S. y en su caso la autorización otorgada por el mismo para el uso de dicha información.-

Que, en contestación al oficio remitido por el Juzgado, la Firma INFORMCONF S.A., ha enviado informe sobre los datos personales y antecedentes de carácter financiero del Sr. L. R. S. con C.I. Nº 656.032, menciona el representante legal de la citada firma que: "… mi conferente si bien se allana oportunamente a la corrección de algún dato falso o erróneo de los informes de la actora, rechaza en forma categórica esta acción y todo lo manifestado por la adversa. En efecto, la parte accionante parece no tener en cuenta que posee cinco DEMANDAS PENDIENTES, INHIBICIONES, REMATES PENDIENTES, VARIAS MOROSIDADES PENDIENTES que figuran en los informes comerciales de la misma, por lo que mal puede se catalogado de un dato falso, en cuanto a las demandas pendientes, debe acercarnos los finiquitos de las mismas de conformidad a la ley 1682/2001 que en su art. 7 establece la necesidad que los particulares concurran a nuestras oficinas a actualizar sus datos y a la ley 1909/2002 modificatoria de la anterior para poder cargarlos en la base de datos de nuestra empresa y finiquitar las demandas pendientes. No podemos mentir y tener en nuestra base de datos algo que no está finiquitado por nuestros afiliados, todos ellos trabajadores del crédito. El actor de la presente acción, no presentó al Juzgado ningún otro finiquito o recibo de pago..//.. de todo lo expuesto y en contraposición a lo manifestado por la adversa, concluimos que la única autorización requerida es aquella referente a la inclusión del afectado en este caso de la actora, en la base de datos en calidad de Moroso (si lo estuviera) es responsabilidad de la empresa financiera o comercial afiliada a mi representada de conformidad a lo establecido por el art. 5º de la Ley 1682/2001…". Finalmente la parte accionada concluyó su contestación solicitando el rechazo con costas de la acción del Habeas Data por improcedente.-

Que, la Garantía Constitucional del Habeas Data se halla consagrada el art. 135 de nuestra Carta Magna la cual dispone que: *"Toda persona puede acceder a la información y a los datos que sobre si misma o sobre sus bienes que obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado*

competente la actualización, la rectificación o la destrucción de aquellos si fuesen erróneos o afecten ilegítimamente sus derechos

Que, frente a Principio constitucional enunciado nos encontramos con la Ley 1682/2001 "QUE REGLAMENTA LA INFORMACIÓN DE CARÁCTER PRIVADO", modificada por Ley Nº 1969/2002, que en virtud a lo dispuesto en su art. 1º, en primer término delimita el objeto de dicha ley, mencionando que regula la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y en general el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares. En igual sentido el art. 2º establece el derecho que tiene toda persona a recolectar, almacenar y procesar datos personales para uso estrictamente privado, además de que las fuentes públicas de información son libres para todos, con las limitaciones previstas por el artículo 5º de dicha ley que dice lo siguientes: *"Los datos de personas físicas o jurídicas individualizadas, que revelen, describan o estimen su situación patrimonial, solvencia económica o al cumplimiento de sus obligaciones comerciales, podrán ser publicados o difundidos, solamente: a) Cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente; b) cuando se trate de informaciones o calificaciones que entidades estatales o privadas deban publicar o dar a conocer en cumplimiento de disposiciones legales específicas, y c) cuando consten en las fuentes públicas de información.* Asimismo, el artículo 6º establece: *"Pueden ser publicados y difundidos: a) Los datos que consistan únicamente en nombre y apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional; b) Cuando se trate de datos solicitados por el propio afectado; y, c) Cuando la información sea recabada en el ejercicio de sus funciones por magistrados judiciales, fiscales, comisiones parlamentarias o por otras autoridades legalmente facultadas para tal efecto".-*

Que, pasando al estudio de la acción planteada, de acuerdo al informe remitido por la firma INFORMCONF S.A., el Sr. L. R. S. registra cuatro demandas y un remate pendiente en distintos Juzgados, además de una demanda finiquitada, con el levantamiento de la inhibición impuesta dentro del mismo proceso. Dicha situación según manifestaciones del accionante lo produce un gran daño no sólo moral, sino también político y patrimonial que afecta su buen nombre, honor y reputación como ciudadano paraguayo así como también en sus actividades comerciales, crediticias, financieras, sociales, laborales y políticas cotidianas, con la consecuente violación de sus derechos previstos en la Constitución Nacional.-

Que, teniendo en cuenta los presupuestos exigidos por la normativa constitucional, tenemos que el accionante no ha referido que la información sobre su persona proporcionada por INFORMCONF sea errónea, por el contrario ha admitido la existencia de tales demandas pendientes. El accionante tampoco ha demostrado que dicha información sobre su persona afecta ilegítimamente sus derechos, puestos que la firma INFORMCONF, ha obtenido dichos datos de las fuentes públicas de información (Sección Estadísticas de los Tribunales, art. 10 de la Ley Nº 805/1996, modificada por Ley Nº 3711/2009).-

Que, en ese sentido, tampoco se puede hablar de una afectación ilegítima de sus derechos, en atención a lo previsto por la LEY 1682/2001 "QUE REGLAMENTA LA INFORMACIÓN DE CARÁCTER PRIVADO", modificada por Ley 1969/2002, la cual en su art. 5º determina concretamente los casos en que las personas, empresas o entidades que suministran información podrán publicar o difundir datos de personas físicas o jurídicas individualizadas, que revelen, describan o estimen su situación patrimonial, solvencia económica o el cumplimiento de sus obligaciones comerciales, sin necesidad de orden judicial alguna que lo disponga. Tales casos se dan: a) Cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente; b) cuando se trate de informaciones o calificaciones que entidades estatales o privadas deban publicar o

dar a conocer en cumplimiento de disposiciones legales específicas; y c) Cuando consten en las fuentes públicas de información. Por su parte, el art. 6º de dicha ley, también enumera los casos en que se podrá publicar o difundir la información registrada en la base de datos de las empresas o entidades que se dedican a tal actividad, consistentes en *datos personales públicos* (nombre y apellido, documento de identidad domicilio, ocupación, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono de ocupaciones, etc.), También cuando se trate de datos solicitados por el propio afectado; y por último cuando magistrados judiciales, fiscales, comisiones parlamentarias o por otras autoridades legalmente facultadas para ese efecto, recaben la información en el ejercicio de sus funciones. Por lo tanto, hallándose claramente previstos en nuestro ordenamiento legal, los casos en que se halla autorizada la publicación y difusión de datos personales, no se justifica la existencia de una resolución judicial que así lo ordena a la empresa o entidad que se dedica a tal actividad.-

En este orden de normativas, se advierte que la firma INFORMCONF S.A., adecua plenamente la información obrante en sus archivos, a las normativas constitucionales y leyes reglamentarias del art. 135 de la Constitución Nacional, por lo que a criterio de esta Magistratura corresponde rechazar la acción de HABEAS DATA planteada por el Sr. L. R. S. con C.I. Nº 656.032 contra la Firma INFORMCONF S.A.-

En cuanto a las costas, este Juzgado considera que al no ser advertida la existencia de mala fe en el planteamiento de la parte actora, puesto que la presentación del Hábeas Data que es una Garantía Constitucional, ha originado la remisión de un informe al Juzgado por la parte demandada, que en nada agravia a las partes, por lo que corresponde a derecho imponer las costas en el orden causado.-

POR TANTO, en base a las consideraciones que anteceden y a las normas constitucionales legales enunciadas, el Juzgado:-

R E S U E L V E:

NO HACER LUGAR a la acción de HABEAS DATA planteada por el Sr. L. R. S. con C.I. Nº 656.032 contra la Firma INFORMCONF S.A., por improcedente, conforme a lo expuesto en el considerando de la presente resolución.-

IMPONER LAS COSTAS en el orden causado.-

ANOTAR, registrar, notificar y remitir copia a la Excma. Corte Suprema de Justicia.-

Firmado: Lici Ma. Teresita Sánchez, Juez Penal de Sentencia
Ante mi: Cynthia Giménez Ibarrola, Actuaria Judicial

TRIBUNALES DE APELACIÓN

JUICIO: "C. A. R. c/ INFORMCONF (INFORMES CONFIDENCIALES) s/INDEMNIZACIÓN DE DAÑOS Y PERJUICIOS".-

ACUERDO Y SENTENCIA NÚMERO: CIENTO OCHENTA Y UNO.

En Asunción, Capital de la República del Paraguay, a los doce días del mes de diciembre del año dos mil siete, estando reunidos en la Sala de Acuerdos del Excmo. Tribunal de Apelación en lo Civil y Comercial, *QUINTA SALA,* los señores Miembros Magistrados FREMIORT ORTIZ PIERPAOLI, CARMELO A. CASTIGLIONI Y LINNEO YNSFRAN SALDIVAR, bajo la presidencia del primero de los nombrados y por ante mí el Secretario autorizante, se trajo para acuerdo el expediente titulado como más arriba se menciona, a fin de resolver los recursos de nulidad y apelación interpuestos contra la S.D.N° 416 de fecha 02 de agosto de 2007, dictada por la Juez de Primera Instancia en lo Civil y Comercial del Cuarto Turno, de esta Capital.-

Previo estudio de los antecedentes del caso, el Tribunal resolvió plantear y votar las siguientes;

CUESTIONES:

ES NULA LA SENTENCIA APELADA?-
SE DICTO ESTA CONFORME A DERECHO?-

Practicado el sorteo de Ley resultó el siguiente orden de votación: CARMELO A. CASTIGLIONI, LINNEO YNSFRAN SALDIVAR Y FREMIORT ORTIZ PIERPAOLI.-

A LA PRIMERA CUESTIÓN PLANTEADA EL MAGISTRADO CARMELO A. CASTIGLIONI DIJO: Este recurso fue interpuesto contra la S.D.N° 416 de fecha 02 de agosto de 2007, que fue expresamente desistido, y al no constatarse vicio alguno que amerite la nulidad de oficio, debe tenerse por desistido de este recurso al recurrente. Es mi voto.-

A SUS TURNOS los Miembros Magistrados LINNEO YNSFRAN SALDIVAR y FREMIORT ORTIZ PIERPAOLI, manifestaron adherirse al voto precedente por los mismos fundamentos.-

A LA SEGUNDA CUESTIÓN PLANTEADA EL MIEMBRO DR. CARMELO A. CASTIGLIONI PROSIGUIO DICIENDO: Se agravia el apelante contra la S.D.Nº 416 de fecha 02 de agosto de 2007, que resolvió: hacer lugar a la demanda de indemnización de daños y perjuicios, promovida por el señor C. A. R. contra INFORMCONF derivado de una publicación de datos por la empresa demandada, proveedora de datos confidenciales al comercio en general.-

El apelante no objeta la existencia del hecho, solo alega que no ha demostrado cabalmente por el actor, de manera que la jueza haya podido inferir efectivamente ha existido ese hecho y consumado la injuria alegada. Dice también que: "NO SE HA EVIDENCIADO LA MAGNITUD DE LA ALTERACIÓN DEL BIENESTAR DEL AFECTADO, PARA QUE ELLA SEA VIABLE? Lo esencial para resolver esta cuestión nos remite a la expresión utilizada por el propio apelante al decir textualmente cuanto sigue: "MI MANDANTE, SI BIEN PUDO COMETER UN ERROR, NO PUDO CAUSARLE UN DAÑO MORAL DE LA MAGNITUD ESTIMADA, Y ESE PERJUICIO DEL CUAL SE HABLA EN TODOS LOS FALLOS Y OPINIONES, COMO ES SABIDO DEBE SER ANTE TODO REAL Y CIERTO". La transcripción es suficiente para resolver el caso, pues el reconocimiento del error es categórico, solo objeta la magnitud estimada como daño moral. El perjuicio dice, además, debe ser real y cierto.-

Entrando a estudiar el caso, constatamos que el error ha sido admitido y debe aplicarse el Art. 289 del C.C., en cuya virtud "EL ERROR NO PERJUDICA CUANDO HA HABIDO RAZÓN PARA ERRAR, PERO NO PODRÁ SER ALEGADO CUANDO PROCEDIERE DE NEGLIGENCIA IMPUTABLE". No se demostró que haya habido razón para errar y sin embargo esta demostrada la negligencia imputable, pues la naturaleza del trabajo de proveer informaciones al público, requiere de extrema prudencia y cuidado, y al no obrar de esa forma la negligencia de proveer informaciones erradas le

resulta imputable. Con esto está probada la antijuricidad, y la relación causal no esta negada y además reconocida en forma expresa. El factor de atribución es la culpa como negligencia, por lo expresado. En cuanto al daño dice el apelante que este debe ser real y cierto. Establece el art. 249 del C.P.C., que: "los hechos notorios no necesitan ser probados; la calificación de los mismos corresponde al Juez". En este caso es notorio el perjuicio a la imagen por tratarse de datos falsos dados a publicidad. Resulta notorio que una información falsa sobre la personalidad, como decir que se debe lo que no se debe y, además, tener carácter público la provisión de esa información, el daño a la imagen es evidente. Y este daño es intangible porque la imagen es un bien jurídico inmaterial y no puede demostrado por una prueba material. Por otra parte el art. 372 del C.C. es por demás claro al establecer que "el ejercicio abusivo de los derechos no esta amparado por la ley y compromete la responsabilidad del agente por el perjuicio que cause (…)cuando contradiga los fines que la ley tuvo en mira reconocerlos". Complementa al artículo trascripto el art. 421 del C.C., que dice: EL DEUDOR RRESPONDERÁ POR LOS DAÑOS Y PERJUICIOS QUE SU DOLO O CULPA IRROGARE AL ACREEDOR. HABRA CULPA CUANDO OMITIEREN AQUELLAS DILIGENCIAS EXIGIDAS POR LA NATURALEZA DE LA OBLIGACIÓN Y CORRESPONDAN A LAS CIRCUNSTANCIAS DE LAS PERSONAS, TIEMPO Y LUGAR". En este caso hubo omisión en la diligencias exigidas por la naturaleza de la obligación, ser cauto y prudente en la provisión de informaciones. El 1835 establece que "EXISTIRA DAÑO SIEMPRE QUE SE CAUSARE A OTRO ALGUN PERJUICIO EN SU PERSONA, (en este caso la imagen) EN SUS DERECHOS O FACULTADES LA OBLIGACIÓN DE REPARAR SE EXTIENDE A TODA LESION MATERIAL O MORAL". En este caso el daño se manifiesta por el hecho exterior susceptible de ocasionarlo, pues proporcionar datos falsos al público crea un descrédito en el prestigio de la persona y cuando este es que depende de su fama, como es un abogado, que es el caso de autos, el daño moral existe. El daño moral no es el daño material ni se infiere de éste. Ambos son autónomos, puede haber daño moral sin que exista material y es suficiente prueba de haberlo ocasionado del daño el haber realizado un acto ilícito como es dar a publicidad datos que no se ajustan a la realidad y que puede perjudicar el crédito público. Por

otra parte, el monto del mismo, si no se demuestra que debe ser inferior no es suficiente para decir que no existe. Ha demostrado el demandante que tiene trabajado de abogados de mucha importancia y la publicación de esos datos puede afectar la credibilidad del mismo como profesional y eso es un daño moral. Por otra parte, al depender del daño material, la fijación del monto esta discreción del Juez y, por tanto, debe confirmarse la resolución recurrida.-

Siendo así, debe confirmarse con costas a la perdidosa la S.D.N° 416 de fecha 02 de agosto de 2007. Es mi voto.-

A SUS TURNOS los Magistrados LINNEO YNSFRAN SALDIVAR y FREMIORT ORTIZ PIERPAOLI, manifestaron adherir al voto precedente por los mismos fundamentos.-

Con lo que se dio por terminado el acto, firmando los Señores Miembros de conformidad, todo por ante mí de que certifico, quedando acordada la sentencia que sigue de inmediato.-

SENTENCIA NÚMERO: 181

Asunción, 12 de diciembre de 2007

VISTO: Lo que resulta de la votación que instruye el acuerdo precedente y sus fundamentos, el Tribunal de Apelación en lo Civil y Comercial, *QUINTA SALA;*

RESUELVE:

1.- DECLARAR DESIERTO, el recurso de nulidad.
2.- CONFIRMAR, la S.D.N° 416 de fecha 02 de agosto de 2007, por las razones señaladas.
3.- LAS COSTAS, a la perdidosa.-
4.- ANOTAR, registrar, notificar y remitir copia a la Excma. Corte Suprema de Justicia.-

JUICIO: "C. E. R. R. c/ INFORCONOF S/ HABEAS DATA".-

ACUERDO Y SENTENCIA NUMERO: CIENTO UNO

En la Ciudad de Asunción, Capital de la República del Paraguay, a catorce días del mes de octubre de dos mil nueve, reunidos los Miembros de la Segunda Sala del Tribunal de Apelación en lo Civil y Comercial, JUAN CARLOS PAREDES BORDON, MARIA SOL ZUCOLLILLO GARAY DE VOUGA Y GERARDO BAEZ MAIOLA, bajo la presidencia del primero de los nombrados, por ante mí la Actuaria Autorizante se trajo a acuerdo el expediente individualizado antecedentemente a fin de resolver los recursos de apelación y nulidad interpuestos contra la S.D..Nº 796 de fecha 31 de octubre de 2008, dictado por el Juzgado de Primera Instancia en lo Civil y Comercial Cuarto Turno.-

PREVIO estudio de los antecedentes, el Tribunal resolvió plantear y votar las siguientes:

C U E S T I O N E S:

ES NULA LA SENTENCIA APELADA?
EN CASO NEGATIVO, ESTA AJUSTADA A DERECHO?

PRACTICADO el sorteo, resultó que debían votar los Señores Miembros en el siguiente orden: PAREDES BORDON, BAEZ MAIOLA y ZUCCOLILLO GARAY DE VOUGA.

A LA PRIMERA CUESTIÓN EL DR. BAEZ MAIOLA DIJO, el recurrente no funda el recurso y dado que tampoco se advierten vicios que ameriten el pronunciamiento de oficio, corresponde declararlo desierto en atención a lo dispuesto en el artículo 419 CPC.

A SUS TURNOS LOS DRES. ZUCOLILLO GARAY DE VOUGA y PAREDES BORDON votaron en igual sentido.

A LA SEGUNDA CUESTIÓN EL DR. BAEZ MAIOLA PROSIGUIÓ DICIENDO, por medio de la S.D.Nº 796 de fecha 31 de octubre de 2008, el Juzgado de Primera Instancia Civil y Comercial del Cuarto Turno, hizo lugar a la demanda de habeas data promovida por C. E. R. R., contra la firma INFORCONF S.A., y en consecuencia ordenó la supresión del registro de operación morosa declarada por la firma afiliada a INFORCONF S.A., CYMAR & ASOCIADOS Y TERESA ROMAN GENES.

Esta resolución causa agravio a la firma accionada, sosteniendo que si bien en la instancia previa se allanó a la demanda de habeas data, ahora se opone a lo resuelto por dicha resolución, fundada en que la actora ya al tiempo de la promoción de la demanda, registraba en sus archivos una operación morosa y una demanda pendiente con la Cooperativa Universitaria Ltda.. En este sentido, afirma que lo que la adversa debía hacer era cancelar su deuda, pedir el finiquito y esperar se cumplan los plazos respectivos, esgrimiendo que por la Ley 1682/2001, podía publicar antecedentes sin previa autorización de la persona afectada.

Revisadas constancias procesales surge que C. E. R. R., promovió juicio de habeas data contra la empresa INFORCONF S.A., por haber publicado asiento, en sus registro de una supuesta operación impaga que la actora tenía con al firma CYMAR & ASOCIADOS y TERESA ROMAN GENES. Al respecto sostuvo que no existía demanda ni reclamación judicial en su contra, peticionando en consecuencia, la destrucción sin más trámites de cualquier información que tenga o tuviere sobre su persona la citada empresa, como asimismo, que se abstenga de proveer información de cualquier índole a empresas o personas particulares, bajo pena de incurrir en responsabilidad de ley.

Por su parte, la firma INFORCONF contestó demanda (f. 24), afirmando que en virtud a la Ley Nº 1682/2001, estaba autorizada para la divulgación de los antecedentes financieros de la actora que figurasen en fuentes públicas de información, alegando que tal ley establece los plazos y condiciones en que debe permanecer la información financiera. No obstante, formuló oportuno, liso e

incondicional allanamiento a la demanda, para el caso de existir alguna modificación que altere los datos de la recurrente.

En el presente caso, la única cuestión gira en torno a establecer si la divulgación de la información por parte de la firma INFORCONF S.A. respecto a una operación morosa de la actora, fue suministrada en violación a la ley, ya que lo relativo al registro de datos de la supuesta demanda de la Cooperativa Universitaria Ltda. contra la actora, no fue objeto de la demanda.

En este entendimiento, cabe señalar que el Habeas Data constituye una garantía constitucional consagrada en el artículo 135, que tiene como objetivos: el acceder a la información sobre la persona o bienes, conocer el uso que se hace de ellos y su finalidad, pudiendo el interesado pedir al magistrado competente la actualización, rectificación o la destrucción de aquellos si fuesen erróneos o afectaran sus legítimos derechos.

Por su parte, la Ley N° 1969/2002 (QUE ODIFICA, AMPLIA Y DEROGA VARIOS ARTÍCULOS DE LA LEY N°1682/2001 "QUE REGLAMENTA LA INFORMACIÓN DE CARÁCTER PRIVADO" establece su artículo primero que: *"Los datos de personas físicas o jurídicas que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales y financieras, podrán ser publicados o difundidos solamente: a) Cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente…"* (sic).

De conformidad a lo dispuesto en la citada ley, surge que si bien las empresas encargadas de la difusión de datos no requieren autorización expresa para publicar información que obre en registros oficiales, no ocurre lo mismo para los datos relativos al cumplimiento de obligaciones no reclamadas judicialmente. En efecto, en este caso la ley obliga a la empresa a obtener una autorización expresa y por escrito de la persona física o jurídica afectada por la divulgación.

En la especie, surge que al ser lo publicado una información sobre el incumplimiento de la obligación no reclamada judicialmente, la presentación de la autorización se constituía en una condicionamiento para la difusión y en consecuencia, al no haber presentado la demandada ningún documento en demostración de tal autorización, correspondía hacer lugar a la acción y en consecuencia, ordenar la supresión del registro de la operación morosa, declarada por la afiliada a INFORCONF S.A., CYMAR & ASOCIADOS Y TERESA ROMAN GENES, y en consecuencia, confirmar la resolución que así lo dispuso.

En cuanto a las costas, las mismas deben ser impuestas a la recurrente en atención a lo dispuesto en el artículo 203 inc a) CPC.

A SU TURNO LA DRA. ZUCOLILLO GARAY DE VOUGA manifiesta que se adhiere al voto del Dr. Paredes Bordón por los mismos fundamentos.

A SU TURNO EL DR. PAREDES BORDÓN DIJO, Adhiere al voto del conjuez preopinante y agrega, que el recurso solo se ha dirigido respecto de la inclusión en los registros de la firma demandada de la morosidad con CYMAR Y ASOCIADOS y TERESA ROMAN genes, de modo que la firma podrá seguir informando sobre el reclamo judicial, sin hacer mención a la anotación cuya supresión se dispone. Tampoco podrá formular observaciones sobre la actora ni negarse a dar información sobre otras operaciones.

Con lo que se dio por terminado el acto, firmado los Señores Miembros, por ante mí quedando acordada la sentencia que sigue a continuación.

S E N T E N C I A Nº 101

Asunción, 14 de octubre de 2009

VISTO: por mérito que ofrece el acuerdo precedente y sus fundamentos, el Tribunal de Apelación en lo Civil y Comercial, Segunda Sala.

R E S U E L V E:

DECLARARLO DESIERTO el recurso de nulidad.

CONFIRMAR la S.D.Nº 796 de fecha 31 de octubre de 2008.

ANOTAR, registrar y remitir copia a la Excma. Corte Suprema de Justicia.

Firmado: Juan Carlos Paredes Bordón, María Sol Zuccolillo de Vouga y Gerardo Báez Mamola.
Ante mí: María Teresa Cañete, Actuaria Judicial

CORTE SUPREMA DE JUSTICIA

EXPEDIENTE: "N. S. y OTROS c/ ENTIDAD BINACIONAL YACYRETA S/ AMPARO CONSTITUCIONAL DE PRONTO DESPACHO".-

ACUERDO Y SENTENCIA NÚMERO QUINIENTOS VEINTE Y NUEVE

En Asunción del Paraguay, a los seis días del mes de diciembre del año mil novecientos noventa y seis, estando en la Sala de Acuerdos de la Corte Suprema de Justicia, los Excmos. Señores Ministros de la Sala Constitucional, Doctor RAUL SAPENA BRUGADA, Presidente y Ministros, Doctores OSCAR PACIELLO CANDIA y LUIS LEZCANO CLAUDE, ante mí, el Secretario Autorizante, se trajo al acuerdo el expediente caratulado: "N. S. y otros c/ Entidad Binacional Yacyretá s/ amparo constitucional de pronto despacho", a fin de resolver el recurso de apelación deducido por el Dr. P. M. P. contra la Sentencia Definitiva No 335 de fecha 31 de agosto de 1994, recaída en autos

Previo estudio de los antecedentes del caso, la Corte Suprema de Justicia, Sala Constitucional, resolvió plantear y votar la siguiente.-

C U E S T I Ó N:

¿Es procedente el recurso de apelación deducido?-

A la cuestión planteada, el Doctor LEZCANO CLAUDE dijo: "Por la vía de la apelación de la S.D. Nº 335, de fecha 31 de agosto de 1994, dictada en primera instancia, llegó este expediente a consideración de la Corte Suprema de Justicia .-

Previamente, debemos referimos a la solicitud de declaración de caducidad de la instancia presentado por los actores, quienes aducen que ha transcurrido el plazo de ley sin que ninguna de las partes impulsara en procedimiento durante dicho lapso. Fundamentan su petición en lo dispuesto en los artículos 172 y si

entes del Código Procesal Civil, y también en la doctrina y la jurisprudencia aplicables al caso.-

El juicio en estudio está pendiente de resolución y de conformidad con el artículo 176 del código de forma, la caducidad no se producirá cuando los procesos estuvieron pendientes de alguna resolución y la demora en dictarla fuere imputable al juez o tribunal. Por ende, el pedido de caducidad formulado por los amparistas no es procedente.-

Corresponde ahora pronunciarse sobre la apelación interpuesta, a pesar de que lo más probable es que el fallo resulte de poca o ninguna utilidad práctica, sea porque ya se consumaron los hechos que motivaron o la promoción del juicio, no siendo ésta una vía idónea para obtener algún tipo de reparación; sea porque las partes hayan solucionado el litigio de otro modo.-

En realidad, el recurso de apelación interpuesto por la parte demandada debió haber sido declarado desierto, pues el escrito de expresión de agravios no reúne los requisitos mínimos para ser aceptado, según lo exige el artículo 419 del Código Procesal Civil. El apelante se limitó a reproducir las mismas alegaciones vertidas en el momento de contestar la demanda, sin analizar la resolución recurrida y exponer los motivos que tenía para consideraría injusta o viciada.-

En el primer punto de la sentencia apelada, el A-quo ha declarado la inconstitucionalidad del artículo XIX del Tratado de Yacyretá que establece que Asunción es la jurisdicción competente para resolver los conflictos derivados de su aplicación. Tal disposición se halla en discordancia con el carácter breve, sumario y gratuito, que según la Constitución (artículo 134), debe tener el amparo. Por tanto, cualquier norma jurídica de inferior jerarquía que lo distorsione, resulta inconstitucional.-

El razonamiento seguido por el A-quo nos parece correcto. En efecto, sustanciar en Asunción un juicio de amparo por conflictos suscitados en Encarnación equivaldría a desvirtuar todos

los plazos sumarios característicos de este tipo de juicio, debido a la ampliación de los términos por razón de la distancia, e igualmente contribuiría a encarecer todos los costos, si se tiene en cuenta que para la substanciación de m juicio de amparo se requiere reunir a las partes en una audiencia de conciliación, y que, generalmente, en este juicio es muy importante la inspección ocular. Estos factores traerían aparejadas la conversión del amparo en un juicio ordinario, con lo cual las bondades de este instituto se desvanecerían, convirtiéndose en letra muerta una de las garantías constitucionales de la más alta relevancia. Por ello consideramos acertada la decisión del juez de primera instancia de no hacer lugar a la excepción de incompetencia de jurisdicción, contenida en el punto dos de la sentencia apelada.-

Así mismo, consideramos que, como se planteó, correspondía el amparo, y no el Hábeas Data. En efecto, no se trataba simplemente de “acceder a la información y a los datos" que sobre el peticionante o sobre sus bienes obraran "en registros oficiales o privados de carácter público..." (artículo 135) , si no de ordenar a la demandada la realización de una acción determinada, cuyo resultado sería una información nueva, no existente en el momento de la promoción de la acción. Pensamos también que se hallaban reunidos los presupuestos indispensables para la procedencia de la acción de amparo, por lo que el punto tres de la sentencia recurrida resulta igualmente correcto.-

Por las razones apuntadas, consideramos que el fallo apelado debe ser confirmado, con imposición de costas a la perdidoso.-

A su turno los Doctores SAPENA BRUGADA Y PACIELLO CANDIA manifestaron que se adhieren al voto del Ministro preopinante, Doctor LEZCANO CLAUDE por los mismos fundamentos.-

Con lo que se dio por terminado el acto firmado S.S.E.E., todo por ante mí que lo certifico quedando acordada la sentencia que inmediatamente sigue:

SENTENCIA NUMERO Nº 529

Asunción, 6 de diciembre de 1996

VISTO: Los méritos del Acuerdo que antecede, la
CORTE SUPREMA DE JUSTICIA
Sala Constitucional
RESUELVE:

1) CONFIRMAR la sentencia definitiva Nº 335, de fecha 31 de agosto de 1.994, dictada por el Juez de Primera Instancia en lo Civil, Comercial y Laboral de la Circunscripción Judicial de Encarnación.-

2) IMPONER las costas a la perdidosa.-

3) ANOTAR, registrar y notificar -

ACCION DE INCONSTITUCIONALIDAD EN EL JUICIO: "ESTABLECIMIENTOS PACU CUA S.R.L. C/ ENTIDAD BINACIONAL YACYRETA S/ HABEAS DATA".-

ACUERDO Y SENTENCIA NUMERO CUATROCIENTOS SETENTA Y SIETE

En Asunción del Paraguay, a los un día del mes de setiembre del año mil novecientos noventa y siete, estando en la Sala de Acuerdos de la Corte Suprema de Justicia, los Excmos. Señores Ministros de la Sala Constitucional, Doctor, LUIS LEZCANO CLAUDE Presidente y Ministros, Doctores: OSCAR PACIELLO CANDIA y RAUL SAPENA BRUGADA, ante mí, el Secretario Autorizante, se trajo al acuerdo el expediente caratulado: "ESTABLECIMIENTOS PACU CUA S.R.L. C/ ENTIDAD BINACIONAL YACYRETA S/ HABEAS DATA", a fín de resolver la acción de inconstitucionalidad promovida por el Ab. Atilio Gómez Grassi.-

Previo estudio de los antecedentes del caso, la Corte Suprema de Justicia, Sala Constitucional, resolvió plantear y votar la siguiente:-

C U E S T I O N :

Es procedente la acción de inconstitucionalidad deducida

A la cuestión planteada, el Doctor PACIELLO CANDIA dijo: "1.- Que se presenta el representante convencional de la Entidad Binacional Yacyretá e impugna de inconstitucionalidad las sentencias Nº 179 y Nº 45, dictada, la primera, por el Juez de Primera Instancia y la segunda por el Tribunal de Apelación, ambas de la Circunscripción Judicial de Itapúa en los autos "Establecimientos Pacú Cuá S.R.L. c/ Entidad Binacional Yacyretá s/ Habeas Data".-

2.- Cuanto cuestiona la entidad de referencia hace relación primero a la incompetencia de la jurisdicción y en segundo lugar al

procedimiento impreso para la sustanciación de este recurso. Por su parte, la entidad accionada en esta acción de inconstitucionalidad, deduce por vía de defensa la excepción de inconstitucionalidad en relación con el artículo XIX del Tratado de Yacyretá.-

3.- Corresponde, por tanto, ocuparse en primer término de la excepción. El tratado en cuestión establece que la jurisdicción competente serán la ciudad de Asunción y Buenos Aires. El excepcionante expresa que esta es una norma inconstitucional, discriminatoria, en cuanto a que obliga a habitantes de Itapúa, por ejemplo, a tener que trasladarse a Asunción para la hipótesis de tener que deducir cualquier reclamo contra la mencionada entidad.-

En puridad de verdad, para la hipótesis planteada por el excepcionante, no se trataría sino de una prórroga de la competencia territorial, perfectamente lícita aún en el orden de las relaciones privadas ordinarias. Esto, desde luego, no merece mayores comentarios y menos tratándose de un Tratado Internacional. Las Altas Partes contratantes de tal acto internacional así lo han creído oportuno en ejercicio de su soberanía, de suerte que mal podría darse ninguna cuestión constitucional a su respecto.-

Corresponde, a mi entender, el rechazo con costas de la excepción articulada con carácter previo.-

4.- Por la razón apuntada, de inicio tenemos que habiéndose substanciado la cuestión ante juzgado y tribunal incompetentes, todo el procedimiento deviene contrario a las reglas del debido proceso legal, razón por la que no cabe otra alternativa que hacer lugar, con costas, a la presente acción, tal cual lo aconseja el Fiscal General del Estado.-

5.- Finalmente, no quiero eludir la cuestión de fondo. El Habeas Data no es el medio lícito para preconstituir pruebas utilizables en un proceso ulterior. Frente al derecho de cualquier

ciudadano de borrar, enmendar o rectificar datos, que obren en un registro público o privado de carácter público, está el principio de inviolabilidad del patrimonio documental de las personas establecido en el artículo 35 de la Constitución Nacional. Debe entenderse, por lo demás, que los datos que pueden obtenerse por la vía del Habeas Data a los efectos de su rectificación o destrucción por su falsedad, son datos que deben constar en registros públicos o privados de acceso público, pero no cualquier documentación o asiento contable que, cabe reiterarlo, forma parte del patrimonio documental inviolable de las personas.-

Atento a todas las consideraciones que preceden, corresponde hacer lugar, con costas a la presente acción de inconstitucionalidad declarando la nulidad por inconstitucionales de las sentencias recurridas. Así voto.-

A su turno el Doctor LEZCANO CLAUDE dijo: “Me adhiero al sentido del voto del ilustre Ministro preopinante, por lo expresado en el punto 5 del mismo. En la hipótesis de que los fallos impugnados no fueran afectados en su validez, se estaría desvirtuando la esencia del Habeas Data, tal cual está consagrado en el artículo 135 de la Constitución. La adopción de esta decisión por parte de la Corte Suprema encuentra pleno respaldo en lo preceptuado en el artículo 563 del Código Procesal Civil.-

En cuanto a las costas, existiendo dos resoluciones en el mismo sentido que justifican la oposición al progreso de esta acción, considero que deben ser impuestas en el orden causado. Es mi voto.-

A su turno el Doctor SAPENA BRUGADA manifestó que se adhiere al voto del Ministro preopinante, Doctor PACIELLO CANDIA por los mismos fundamentos.-

Con lo que se dió por terminado el acto firmando su SS.EE., todo por ante mí, de que certifico, quedando acordada la sentencia que inmediatamente sigue:

SENTENCIA NUMERO: 477
Asunción, 1 de setiembre de 1997
VISTO: Los méritos del Acuerdo que antecede, la
CORTE SUPREMA DE JUSTICIA
SALA CONSTITUCIONAL
RESUELVE:

HACER LUGAR a la presente acción de inconstitucionalidad, con costas, y en consecuencia, declarar la nulidad de la S.D. Nº 179 de fecha 14 de abril de 1.993, dictada por el Juzgado de Primera Instancia en lo Civil, Comercial, Laboral y Tutelar del Menor de la Circunscripción Judicial de Itapúa y el Acuerdo y Sentencia Nº 45 de fecha 22 de julio de 1993, dictado por el Tribunal de Apelación de la misma circunscripción judicial.-

ANOTAR, registrar y notificar.-

ACCION DE INCONSTITUCIONALIDAD EN EL JUICIO: "M. D. R. C. s/ HABEAS DATA". AÑO: 1997– Nº 307.-

ACUERDO Y SENTENCIA NÚMERO: SETENTA Y DOS

En Asunción del Paraguay, a los quince días del mes de marzo del año dos mil, estando en la Sala de Acuerdos de la Corte Suprema de Justicia, los Excmos. Señores Ministros de la Sala Constitucional, Doctor, CARLOS FERNANDEZ GADEA Presidente y Ministros, Doctores LUIS LEZCANO CLAUDE y RAUL SAPENA BRUGADA, ante mí, el Secretario autorizante, se trajo al acuerdo el expediente caratulado: ACCION DE INCONSTITUCIONALIDAD EN EL JUICIO: "M. D. R. C. s/ HABEAS DATA", a fin de resolver la acción de inconstitucionalidad planteada por M. R. R. C., por sus propios derechos, bajo patrocinio de abogado.

Previo estudio de los antecedentes del caso, la Corte Suprema de Justicia, Sala Constitucional, resolvió plantear y votar la siguiente:-

C U E S T I O N

¿Es procedente la acción de inconstitucionalidad deducida?.-

A la cuestión planteada el Doctor SAPENA BRUGADA dijo: Se presentó ante esta Corte, M. R. R. C., por sus propios derechos, bajo patrocinio de abogado y solicitó la declaración de inconstitucionalidad y consiguiente nulidad del Acuerdo y Sentencia Nº 10 de fecha 13 de mayo de 1997 dictado por el Tribunal de Apelación en lo Criminal, Primera Sala.-

Se trae a estudio de esta Corte un juicio sobre habeas data en el cual M. R. R. C. en nombre y representación de su hija menor M. D. R. C., peticionó la garantía constitucional a fin de obtener "la destrucción de toda la documentación" que diera origen a la inscripción de un certificado de nacimiento en el cual figura como padre de la menor J. M. B. R.-

En primera instancia se ordenó la rectificación del Acta Nº 478/1996 del Registro del Estado Civil en el sentido de suprimir de su contenido la declaración del reconocimiento de filiación y el nombre de J. M. B. R.-

Por la resolución impugnada se declaró la nulidad de la sentencia dictada en la instancia inferior.-

Se presenta ahora ante esta Corte la accionante y alega que la resolución judicial cuestionada por esta vía ha sido dictada en contra de preceptos constitucionales, causando lesiones a los derechos y garantías que la misma confiere, citando los arts. 4, 25 28, 33, 45, 49, 53, 54, 131 y 135 de la Constitución Nacional.-

La presente acción debe ser rechazada. Se pretende por la vía del habeas data extraer de un certificado de nacimiento el nombre del padre con el argumento de que éste carece de la titularidad. La pregunta que surge entonces es si la garantía constitucional puede "alterar" por así decirlo la calidad filial de una persona. El tribunal de apelación consideró que el magistrado se sobrepasó en el ejercicio de sus facultades al haber ordenado la rectificación del acta de nacimiento, pues no es su competencia resolver cuestiones de familia. La accionante se agravia con este argumento del tribunal pues considera que la propia Constitución autoriza a la rectificación o destrucción de la información que no es veraz a través del habeas data. Justamente en el caso en estudio, se trata de un certificado de nacimiento, instrumento de orden público que hace plena fé y cuyas modificaciones deben ser realizas en el juicio correspondiente. De admitirse la posibilidad de enmienda del estado filial de las personas a través de un juicio de habeas data se estaría desnaturalizando este noble instituto y omitiendo otros procesos legales. Conforme a la definición que nos da la propia Constitución en su art. 135 "*Toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos*". De esta definición se

desprende que el habeas data es una garantía para que las personas puedan obtener todos los datos relativos a su persona y si fuesen erróneos o afectaran ilegítimamente sus derechos, pedir como en el presente caso, su destrucción. De las propias manifestaciones de la accionante surge que la paternidad está en discusión por las vías ordinarias. De las resultas de dicho juicio podrá reclamarse la rectificación del certificado de nacimiento y determinarse con exactitud si la inscripción afecta o no ilegítimamente sus derechos. Finalmente, no se detecta en la resolución en estudio transgresiones de carácter constitucional que ameriten la procedencia de esta acción. Voto en consecuencia, por su rechazo.-

Las costas a cargo de la perdidosa.-

A su turno los Doctores LEZCANO CLAUDE y FERNANDEZ GADEA, manifestaron que se adhieren al voto del Ministro preopinante, Doctor SAPENA BRUGADA, por los mismos fundamentos.-

Con lo que se dio por terminado el acto, firmando SS.EE., todo por ante mí, de que certifico, quedando acordada la sentencia que inmediatamente sigue:-

SENTENCIA NUMERO: 72

Asunción, 15 de marzo de 2000
VISTO: Los méritos del Acuerdo que anteceden, la
CORTE SUPREMA DE JUSTICIA
SALA CONSTITUCIONAL
R E S U E L V E:

RECHAZAR la acción planteada.-

IMPONER costas a la perdidosa.-

ANOTAR, registrar y notificar.-

JUICIO: "O. K. L. y OTROS C/UNIVERSIDAD TECNOLÓGICA INTERCONTINENTAL (UTIC) S/HABEAS DATA".-

ACUERDO Y SENTENCIA NÚMERO: CINCO

En Asunción, Capital de la República del Paraguay, a los un días, del mes de febrero, del año dos mil siete, estando reunidos en su Sala de Acuerdos los señores Ministros de la Excelentísima Corte Suprema de Justicia, Sala Civil y Comercial, José Raúl Torres Kirmser, Miguel Oscar Bajac Albertini y César Antonio Garay, bajo la presidencia del primero de los nombrados, Ante mí el Secretario autorizante, se trajo para el Acuerdo el expediente intitulado: "O. K. L. y OTROS C/UNIVERSIDAD TECNOLÓGICA INTERCONTINENTAL (UTIC) S/HABEAS DATA", a fin de resolver los Recursos y Apelación y Nulidad interpuestos contra el Acuerdo y Sentencia Número 28, con fecha 3 de marzo del 2005, y el Acuerdo y Sentencia Número 36, del 14 de Marzo del 2005, dictados por el Tribunal de Apelación en lo Civil y Comercial, Tercera Sala, de la Capital.-

Previo estudio de los antecedentes del caso, la Excelentísima Corte Suprema de Justicia, Sala Civil y Comercial, resolvió plantear y votar las siguientes; -

CUESTIONES:

Es nula la Sentencia apelada?.-
En caso contrario, se halla ajustada a Derecho?.-

A los efectos del juzgamiento de las cuestiones a ser estudiadas y con el objeto de establecer un orden en la emisión de los votos, se procede al sorteo, arrojando el siguiente resultado: MIGUEL BAJAC ALBERTINI, CÉSAR ANTONIO GARAY y RAÚL TORRES KIRMSER.-

A LA PRIMERA CUESTIÓN PLANTEADA, EL DR. MIGUEL OSCAR BAJAC ALBERTINI dijo: El recurso de nulidad no fue fundamentado, por lo que corresponde declararlo desierto, no sin antes advertir que analizadas las resoluciones recurridas, no se

observan vicios o defectos de índole procesal que ameriten declarar la nulidad de oficio, de conformidad con lo dispuesto por los artículos 113 y 404 del Código Procesal Civil.-

A SUS TURNOS LOS SEÑORES MINISTROS CÉSAR ANTONIO GARAY y RAÚL TORRES KIRMSER manifiestan adherir al voto del señor Ministro preopinante por sus mismos fundamentos.-

A LA SEGUNDA CUESTIÓN PLANTEADA, EL MINISTRO MIGUEL OSCAR BAJAC ALBERTINI, prosiguió diciendo: Por el Acuerdo y Sentencia Número 28 de fecha 3 de marzo del año 2005, el A-quem resolvió: "DESESTIMAR el recurso de nulidad; MODIFICAR parcialmente la resolución en los siguientes términos: a) CONFIRMAR en la parte que ordena la expedición de las calificaciones de los recurrentes de acuerdo a los registros obrantes en la institución demandada, b) REVOCAR en la parte que ordena el secuestro de los certificados y legajos de los accionantes; COSTAS por su orden; ANÓTESE…"; y por el Acuerdo y Sentencia No. 36 de fecha 14 de marzo del año en curso, resolvió: "ACLARAR la resolución recurrida, en el sentido de consignar la imposición de costas en el orden causado en ambas instancias; HACER LUGAR a los recursos de aclaratoria respecto del punto a) del apartado segundo de la sentencia recurrida, ordenando la habilitación el la secretaría de la Facultad correspondiente, en el plazo de diez días contados a partir de que la presente resolución quede firme y ejecutoriada, de una carpeta en la cual obren las constancias de las calificaciones, y la puesta a disposición para los accionantes de dicha carpeta en los horarios normales de atención al público de la Universidad; RECHAZAR los recursos de aclaratoria respecto al punto b) del apartado segundo de la sentencia recurrida; ANÓTESE…".-

Contra las sentencias dictadas por el tribunal se alza la parte actora solicitando su revocación, alegando que las mismas afectan notablemente el derecho de sus conferentes para acceder plena y efectivamente a sus certificados de estudios, cuya expedición le es negada en forma arbitraria por los directivos de la Universidad Tecnológica Intercontinental (UTIC). El recurrente asegura que sus representados se sienten perjudicados en sus intereses al negársele

el derecho que tienen de obtener sus certificados de estudios a fin de trasladarse e inscribirse en la institución de su preferencia. La hoy demandada en todo momento negó otorgar los certificados de estudios, situación que perjudica en gran manera a sus poderdantes, al correr el riesgo de perder inclusive el año, y algunos hasta la carrera, ya que no tienen acceso a las documentaciones que les pertenecen y que están siendo retenidas en forma ilegal y arbitraria por las autoridades de la UTIC. Sostiene que sus mandantes nunca tuvieron acceso a la información, inclusive ante los insistentes pedidos presentados en la Facultad, argumentando que tienen obligaciones pendientes de carácter pecuniario con la Universidad, y es por ello que se les niega la entrega de los certificados. Agrega que la lista presentada por la demandada con relación a la situación financiera de alumnos desvinculados en el 2004 (fojas 228/230, 237/239), fue confeccionada en forma arbitraria, irreal e interesada, ya que en ella se limitan a individualizar al alumno y establecer una suma total de la supuesta deuda, sin presentar más documentos que dicha lista, a fin de poner todas las trabas para que no puedan tener acceso a los certificados de estudios. Resalta que sus mandantes con la presente acción no buscan liberarse de obligaciones con la Universidad – en el hipotético caso que las mismas existieran – como se pretende hacer creer, y aclara que sus mandantes buscan que expidan los certificados de estudios, sin que ello implique el desconocimiento de deudas, las cuales, en su caso, deberán ser reclamadas por las vías pertinentes (ordinaria o ejecutiva) y no discutirse en éste tipo de juicios, esencialmente garantista y de carácter sumario. Argumenta además que muchos de sus mandantes se encuentran actualmente en calidad de alumnos condicionales de varias Universidades privadas, pues al no poder contar con los certificados de estudios requeridos, mal pueden acceder a la calidad a la calidad de alumnos regulares, situación absolutamente atentatoria de garantías de rango constitucional como lo constituye el derecho a la educación, por lo que para dicho efecto el artículo 135 de la Carga Magna garantiza el acceso a la información.-

Destaca igualmente que la accionada, en innumerables ocasiones desoyó inclusive la orden judicial emanada del Juzgado de Primera Instancia de exhibir las notas, sin importancia que esto

implique un atentado al mismo Poder Judicial, burlándose inclusive de sus resoluciones. Se pregunta: ¿Qué le llevaría en esta oportunidad a la Cámara? Y en el caso que no la exhiban (como mínimo), ¿cuál es la vía que su parte utilizará para hacer efectivo su derecho de acceder a los certificados de estudios? A todas luces – expresa – estamos frete a resoluciones sumamente peligrosas, ya que antes de garantizar el derecho al acceso a la información por las vías pertinentes, la restringen. Aclara además, que el segundo punto de la S.D.Nº 27, de fecha 10 de febrero de 2005, la cual es revocada por la Cámara, en cuanto a la orden de secuestro de los certificados de estudios, lo único que hace ese hacer efectivo el apercibimiento decretado en autos en las providencias de fecha 29 y 30 de diciembre de 2004, proveídos, que como se podrá notar al examinar los autos, no fueron observados ni recurridos por la accionada, por lo que el Juzgado ordenó el secuestro, ya ante la negativa de la Universidad de expedir de la forma que sea los certificados.-

Finalmente en relación a las costas judiciales sostiene que, al haber sido determinadas por la Cámara de Apelaciones que en todo el juicio sean impuestas en el orden causado, las mismas igualmente son apeladas, solicitando que en las tres Instancias, sean impuestas a la accionada, es decir, universidad Tecnológica Intercontinental (UTIC).-

La adversa contesta solicitando la confirmatoria de las resoluciones apeladas y a dicho efecto rechaza por infundadas y carentes de veracidad las afirmaciones de los actores, en cuanto dicen que la UTIC se niega a otorgarle los certificados de estudios, siendo la verdad de la cuestión que los mismos pretenden desconocer sus obligaciones de las cuotas mensuales por sus estudios en la Universidad, amén del arancel respectivo que también deben abonar por dicha expedición.-

Manifiesta que su parte nunca se ha negado a expedir los certificados de estudios a sus alumnos, y que los actores no han presentados en el juicio recibo de pago alguno que justifique sus reclamos. Asegura que el propósito de los mismos es conseguir los certificados en forma gratuita a través de la garantía constitucional

del Habeas Data, utilizando la función jurisdiccional para tratar de eludir sus pagos. Manifiesta que los actores reconocen que tienen deudas pendientes con la Universidad, y sobre las supuestas pruebas documentales que alegan, dicen que al contestar la demanda ofreció como prueba la pericia contable judicial para verificar la certitud de las deudas de cada uno de los actores, que el Juez de Primera Instancia no hizo lugar, ni lo tubo en cuenta, al no abrir la causa a prueba en el juicio ni declarar la cuestión de puro derecho, en una clara muestra de la irregularidad del juicio. Resalta también que de utilizarse la vía ordinaria o ejecutiva para reclamar el pago de las cuotas atrasadas, como pretenden los apelantes, previo otorgamiento de los certificados de estudios, los Juzgados y Tribunales se llenarán de juicios ejecutivos.-

Sostiene en otro apartado que la pretensión del apelante de apoderarse de documentos en la forma como plantean los actores, no es admitida en la garantía constitucional mencionada, por cuanto que la finalidad de la misma es la actualización, rectificación o destrucción de datos erróneos que afecten sus derechos. En relación al secuestro de los certificados de estudio que fue concedido por el Juez de Primera Instancia, el Juzgado no expidió el mandamiento de secuestro por razones que desconocen, motivo por el cual no pudo cumplirse la disposición y no precisamente por incumplimiento de la UTIC como expresa los apelantes en expresión de agravios. En referencia al abultamiento en forma maliciosa de las cuentas pendientes de los alumnos, la demandada rechaza categóricamente dicho supuesto por ser totalmente infundado y falso, asegurando que en su oportunidad ofreció como prueba la pericia contable judicial. Con respecto a las costas, solicita a la Corte el rechazo de las pretensiones de los actores.-

El art. 135 de la Constitución Nacional dispone “Toda persona podrá acceder a la información y a los datos que sobre sí mismo o sobre sus bienes obren en registro oficiales o privados de carácter público, así mismo conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante magistrado competente la actualización, la rectificación o destrucción de aquellos, si fuesen erróneas o afectaran legítimamente sus derechos”.-

El objeto de ésta Institución es la persona (en su fuero íntimo, en su ámbito privado) y sus bienes (entendido como reserva y completitud), los ciudadanos debemos conocer el uso y destino dado a la información o dato sobre nuestras personas y bienes. Esto nos permite, a través de la garantía constitucional, solicitar ante el órgano judicial competente la ACTUALIZACIÓN, LA RECTIFICACIÓN O SUPRESIÓN de aquellos, considerados erróneos o que afectaren ilegítimamente nuestros derechos. Los términos atizados por la Constitución; "INFORMACIÓN" refiera a la acción y efecto de enterar, instruir, y "DATO" a los antecedentes que permiten llegar más fácilmente a conocimiento de una cosa. Podemos señalar entonces que la procedencia de una acción de Hábeas Data, éste debe necesariamente ajustarse a los siguientes requisitos: a) Debe tratarse de una información y datos sobre las personas o sus bienes; b) La información o datos sobre requeridos deben constar en registros oficiales o privados de carácter público; c) y que el acceso a la información cumpla la finalidad de conocer el uso y destino, para solicitar su actualización, rectificación o destrucción, si ésta información o dato fueran erróneos o afectasen ilegítimamente algún derecho.-

La Corte Suprema de Justicia a través de A.I.N^{o} 649 de fecha 25 de junio de 1996, a falta de Ley reglamentaria, da a conocer su criterio, estableciendo una serie de pautas a ser tenidas en cuenta para la tramitación de éste tipo de acción. Deberá expresar con claridad: a) la identificación del registro de que se trata, b) la expresión del actor de si conoce o no su contenido y en su caso enunciar en que consiste, c) la presentación de prueba u ofrecimiento de probar el error o inexactitud de lo registrado, y d) expresar en que consiste la ilegalidad que afecta al accionado, amén de los enunciados en el art. 215 del C.P.C.. -

En el caso en estudio, los alumnos de la Universidad demandan acceder a los certificados de estudio y legajos. La negativa de la demandada se basa en el hecho de que existen supuestas deudas de los participantes y, hasta tanto no sean saldadas, los certificados de estudios no serán expedidos. Así y conforme a las constancias de autor y a las diligencias realizadas en

los mismos, se debe determinar si el argumento es esgrimido por la demandada es o no válido par que representen un obstáculo al acceso de lo peticionado.-

El bien jurídico protegido lo constituye sustancialmente la veracidad de la información, en lo referente a la persona y sus bienes. En primer lugar se busca proteger a los individuos contra la información falsa o incompleta. Por otra parte, el derecho a la protección de datos tiene la naturaleza de un derecho genérico, significa que esto constituye un plexo de derechos específicos, de los cuales se nutre y recibe su contenido. Estos derechos constituyen el derecho a conocer, el derecho a acceder a los datos o información, y el derecho de rectificar o destruir los mismos. En realidad, lo que preocupa es controlar la veracidad de la información y el uso de que ella se hace.-

Puede interponerla cualquier persona física o jurídica, afectada por la existencia de datos que pudieran ser erróneos, falsos o indebidamente difundidos, debiendo acreditarse prima facie, aunque sea en forma sumaria, el contenido del registro o la constancia que afecte los derechos de los recurrentes. Es de orden público, por lo que, incluso de oficio puede ser deducido. Su objeto primordial según el artículo precedentemente transcripto, es el conocimiento de los datos presumiblemente inexactos existentes en el o en los registros en cuestión.-

El procedimiento del Hábeas Data es esencialmente garantista del derecho a la información, resultando improponible la agregación de cuestiones accesorias a fin de enervar el imperativo constitucional. No debemos sin embargo perder de vista, la necesidad y el deseo de estudio de los recurrentes, que no deben ser privados de dichos certificados por el hecho particular de la deuda, siempre que estos cumplan previamente lo establecido como arancel para la expedición de los documentos requeridos. El certificado de estudios como se dijera, es un documento administrativo que no solo cumple la función de informar las calificaciones obtenidas, sino que permite el acceso a otra Institución de enseñanza. Amén de ello, la expedición de éste

documento está sujeta a un arancel determinado, como se aprecia a fs. 231 y 232.-

En consecuencia, implicaría una desnaturalización del Instituto del Hábeas Data ordenar el secuestro de dichos documentos, dado que así es muy fácil evitar el cumplimiento del pago de los aranceles universitarios pactado y aceptado al momento de la inscripción. Una vez cumplido el trámite administrativo, pago del arancel establecido, la Universidad deberá expedir sin más trámite el certificado correspondiente.-

Recapitulando, el recurso de Hábeas Data tutela el acceso a la información, pero no puede ser vía para evitar el cumplimiento de obligaciones asumidas en virtud de la inscripción y aceptación de los reglamentos de una determinada entidad. Ello debe aclarar el objeto de ésta garantía constitucional, acceso a la información a los efectos de conocer su contenido, y a partir de esa circunstancias exigir las rectificaciones pertinentes.-

Las costas, otro punto de discusión, deben ser impuestas a la vencida. Es mi voto.-

El caso que juzgamos discurre acerca de una Garantía prevista en la Constitución. Y atendiendo ese extremo, la sustanciación fue sui generis, como deben ser aquellas destinadas a proteger generosa y expeditivamente los Derechos que han sido ilegítimamente vulnerados por entidades que poseen registros, datos, calificaciones, certificados de estudios, planillas de exámenes, etc.-

Entre los fundamentos para la interposición del Habeas data se pueden enunciar, a saltos de mata, los que pergeñamos: I) el Derecho a la Información implica que el accionante podrá conocer la existencia de Registro o Bancos de datos de carácter personal, su finalidad y la identidad del responsable; y II) Derecho de Acceso: El interesado tendrá Derecho a solicitar y obtener información de sus datos (carácter personal) que consten en Registros o Bancos de datos públicos o privados destinados a proveer informes para usos que correspondan en Derecho, legítimamente.-

Enrique M. Falcón al comentar las pretensiones que incluye el Habeas Data, ilustra: "En realidad se trata de la regulación de dos pretensiones sucesivas y secuenciales, una subsidiaria de la otra, la primera de información y la segunda de conocimiento y ejecución. La pretensión de información requiere que se trate de: a) datos de un apersona, b) que esos datos consten en registros públicos o privados, y c) que esos registros estén destinados a dar información de los datos del requirente". Cuando explica la razón del nacimiento de este tipo de protección, apunta: "El habeas data es un amparo especializado, importa una configuración especial, procurando la tutela del derecho a tener acceso a la información que de uno tienen los entes públicos o gubernamentales como también los particulares". En el concepto y tipos de los registros leemos: "Un registro es un lugar, archivo, oficina donde se asientan datos. Estos datos se pueden incluir en padrones, protocolos, ficheros, etcétera, y pueden ser manuales o informáticos. Los datos registrados pueden pertenecer a una persona o a una cosa, o a la relación de ambas. Una enumeración genérica nos permite mostrar diversos tipos: 1) Personales (del estado civil, de trabajo, escolares y estudiantiles, bancarios, de mandatos, testamentos, de reincidencia, 0oliciales, militares, etc.)". en lo que concierne a la legitimación pasiva, dice: "El legitimado pasivo es aquel que tiene bajo su custodia el registro o banco de datos, ejerciendo el control de las informaciones físicas o jurídicas, disponibles para los fines respecto de los cuales dichas informaciones son reunidas". De sus conclusiones entresacamos: "2. Su objetivo tiende a que las personas físicas o jurídicas puedan conocer los datos registrados sobre ellas por entidades estatales o privadas, como así también la finalidad de los registros (entendidos éstos en sentido lato de archivos, registro o banco de datos)" (HABEAS DATA. Concepto y Procedimiento, Ed. Abeledo-Perrot, páginas 24 y siguientes).-

La doctrina y jurisprudencia germanas han elaborado una categoría paralela a la libertad informática denominada "derecho a la autodeterminación informativa" (Rect. Auf informationelle Selbstbestimmung). Según la tesis del Tribunal Constitucional (Bundesverfassugsgericht) de Karlsruhe (Sentencia dictada el 15 de diciembre de 1983), el principio básico del ordenamiento jurídico

establecido por la Ley Fundamental de la República Federal de Alemania, es el valor y la dignidad de la persona, que actúa con autodeterminación al formar parte de una sociedad libre. De la dignidad y de la libertad, entendida como autodeterminación, deriva la facultad de la persona de "deducir básicamente por sí misma cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida".-

No le va en zaga el Preámbulo de nuestra Constitución Nacional al reconocer – vasta y formidablemente – "la dignidad humana".-

Miguel Angel Ekmekdjian y Calogero Pizzolo (h.) al comentar aquella estupenda decisión de la Magistratura germana, expresan: "El derecho a la autodeterminación informativa, según el fallo citado, consistiría en la facultad de disponer sobre la revelación y el uso de los datos personales que abarca todas las fases de elaboración y uso de datos, o sea, su acumulación, su transmisión, su modificación y su calificación. Ambas categorías se condicionan mutuamente y representan los dos aspectos de una misma moneda, en este caso en que está en juego un derecho fundamental. La protección de datos carecería de sentido si no se tradujera en un conjunto de galanías para las personas, pero, al propio tiempo, la libertad informática o el derecho a la autodeterminación informativa serían inconcebibles de no contar como presupuesto una opción axiológica más allá del marco organizativo de la información". "El derecho a la protección de datos tiene la naturaleza de un derecho genérico; es decir, constituye un plexo de derecho, que llamaremos específicos, de los cuales se nutre y recibe su contenido. Estos derechos son: el derecho a conocer (right to know), el derecho a acceder (right to access), y el derecho a rectificar (right to correct). El trio de estos derechos es conocido con el nombre de derechos del afectado" (Hábeas data. El derecho a la intimidad frente a la revolución informática, Ediciones Desalma, páginas 24 y siguientes).-

Con sujeción a lo apuntado y de las actuaciones obrantes en el Juicio, se constata que la presentación que juzgamos fue incoada por un grupo de Alumnos de la "Facultad de Derecho de la

Universidad Tecnológica Intercontinental (UTIC)", que solicitaron sus respectivos Certificados de Estudios, los cuales fueron negados por las Autoridades del organismo educacional.-

La intitulada "Facultad de Derecho de la Universidad Tecnológica Intercontinental (UTIC)", en su responde expresó que otorgará las correspondientes Certificaciones de Estudios, con la salvedad que cada Alumno debe estar al día en sus aranceles.-

Prima facie, recordemos el loable propósito de esta Garantía Constitucional, que es facilitar, permitir, propiciar y resolver la obtención de informes obrantes en Instituciones públicas o privadas, que conlleva entregar efectivamente la información requerida, una vez constatados los presupuestos para la viabilidad del Habeas Data, y no como resolvió la alzada al disponer – en el Acuerdo y Sentencia que atendemos ahora – la simple exhibición de las calificaciones. Esta determinación no cumple las entrañables expectativas, objetivos y fines de la Garantía – como máximo rango – en cuestión. Y así como fue resuelto el thema decidendum no alcanzará siquiera para una invocación lírica en los afectados y abusivamente lesionados por el establecimiento que los venía cobijando.-

Conceptuó que se hará efectivo a plenitud el Habeas Data – reitero – no por una simple exhibición de las calificaciones en la denominada "Universidad Tecnológica Intercontinental (UTIC)", insuficiente a los objetivos y fines de quienes han solicitado aquel, como sí mediante la expedición de aquellas, materializadas a través de los Certificados de Estudios, ya que en caso contrario estaríamos propiciando riesgosamente – o al menos cohonestando y facilitando – que prime lo crematístico por encima de valores intrínsecos como son: la Dignidad Humana, que enuncia el Preámbulo de Nuestra Ley Fundamental junto a los Artículos 35, 45, 73, 74, 75 y 135 de la misma; y los que hacen al Demos universitario.-

Refuerzan todavía más estas inexpugnables convicciones jurídicas las enseñanzas que pueden leerse en la obra de Osvaldo Alfredo Gonzaíni, Derecho Procesal Constitucional, HÁBEAS DATA,

Protección de Datos personales, Doctrina y jurisprudencia, Rubinzal Culzoni Editores.-

En las expresadas circunstancias juzgo que el Recurso de Apelación otorgado en el A.I.Nº 1.210, con fecha 7 de julio de 2005, es viable con sujeción a Derecho. Así voto.-

A SU TURNO EL SEÑOR MINISTRO TORRES KIRMSER DIJO: Al promover la acción de esta garantía constitucional de Hábeas Data, radicada en fecha 24 de Diciembre de 2.004, la pretensión de los ex alumnos era la de obtener la efectiva expedición de sus respectivos Certificados de Estudios por parte de las autoridades de la Universidad Tecnológica Intercontinental (UTIC) con el fin de trasladarse e inscribirse en la institución. La falta de expedición de sus respectivos Certificados de Estudios por parte de las autoridades de la Universidad Tecnológica Intercontinental (UTIC) con el fin de trasladarse e inscribirse en la institución de su preferencia, debido a la negativa en otorgarlos por parte de la institución. La falta de expedición de dicho documento por parte de ésta, según los términos de la demanda, les priva del constitucional derecho de aprender al impedirles proseguir regularmente sus estudios universitarios.-

La parte demandada al contestar el traslado manifestó que su decisión de no entregarlos se fundamenta en que existen deudas por parte de los peticionantes y que los documentos no serán expedidos mientras no sean honradas las cuentas.-

Ese es el núcleo central del caso en análisis: la demandada se opone a entregar los certificados a los ex alumnos antes de que los mismos abonen las deudas pendientes y el monto establecido como costo de la expedición de los mismos. Si pagan se les expide; si no pagan no se les expide.-

Tal como lo expresa el Dr. Garay en el voto que antecede y al cual manifiesto mi adhesión, en modo alguno puede admitirse que lo crematístico pudiera primar sobre el constitucional derecho de aprender está expresamente garantizado por la Constitución Nacional en su art. 74. si existieren deudas pendientes a favor de la

UTIC, el ordenamiento jurídico nacional le brinda los mecanismos procesales adecuados para reclamar su cobro. Pero no puede admitirse, en modo alguno, que se utilice el evidente estado de necesidad de los alumnos como un medio para obtener el cobro de sumas de dinero supuestamente debidas.-

La expedición de los certificados luego del pago de las deudas no es una solución útil para los recurrentes, la que sólo será cabalmente satisfecha cuando la demandada efectivamente expida y entregue a los interesados esos certificados, sin perjuicio del derecho que le asiste a la institución de recurrir ante los créditos que eventualmente le correspondiera.-

La retensión de los Certificados de Estudios de los ex alumnos por parte de la demandada es una desobediencia al mandato de protección documental establecido en la Constitución Nacional la que en su art. 35 preceptúa la prohibición de retener los documentos identificatorios, licencias o constancias de las personas, salvo los casos previstos en la ley y en au art. 36 declara inviolable el patrimonio documental de las personas. Ninguna Ley autoriza a la demandada para retener las constancias de los alumnos. Los certificados de estudios son constancias de las personas.-

En mérito al criterio expuesto, al adherir al voto del Ministro Dr. Garay también voto por la revocatoria.-

Con lo que se dio por finalizado el acto, firmado SS.EE., todo por Ante mí de que certifico, quedando acordada la Sentencia que inmediatamente sigue:

ACUERDO Y SENTENCIA NÚMERO: 5

Asunción, 1 de febrero de 2007.-

ACUERDO Y SENTENCIA NÚMERO: 5

Y VISTOS: Los méritos del acuerdo que antecede, la Excelentísima

CORTE SUPREMA DE JUSTICIA
SALA CIVIL Y COMERCIAL
RESUELVE:

DECLRAR Desierto el Recurso de Nulidad.-

REVOCAR el Acuerdo y Sentencia Número 28 del 3 de Marzo de 2005, y su aclaratoria Acuerdo y Sentencia Número 36 con fecha 14 de Marzo de 2005, dictados por el Tribunal de Apelación en lo Civil y Comercial, Tercera Sala, conforme a las motivaciones expuestas precedentemente.-

ORDENAR la inmediata expedición de los Certificados de calificaciones y cuanto más sea menester a los Estudiantes que accionaron, sin ningún condicionamiento previo ni posterior, todo ello en un plazo máximo de cinco días hábiles, improrrogable, una vez quede firme y ejecutoriado este Fallo.-

IMPONER las Costas, de esta Instancia, al vencido.-

Firmado: Miguel Oscar Bajac Albertini, Raúl Torres Kirmser y Antonio Fretes.
Ante mí: Alejandrino Cuevas Cáceres.