

# **El Defensor del Pueblo: Derecho, Tecnologías de la Información y Libertades**

**VICENTE LOPEZ-IBOR MAYOR**

*Abogado.*

**CARMEN PLAZA**

*Licenciada en Derecho.*

## **SUMARIO**

- I) LA FIGURA DEL DEFENSOR DEL PUEBLO Y LA PROTECCION DE LOS DATOS DE CARACTER PERSONAL.
- II) NATURALEZA DEL DERECHO DE PROTECCION A LA AUTODETERMINACION INFORMATIVA.
- III) LA PROTECCION DE DATOS PERSONALES EN EL DERECHO COMPARADO. EL CONVENIO DEL CONSEJO DE EUROPA.

#### **IV) DERECHO COMUNITARIO Y PROTECCION DE DATOS.**

1. La propuesta modificada de Directiva del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos.

2. El Acuerdo de Schengen.

#### **V) LA SENTENCIA DEL TRIBUNAL CONSTITUCIONAL ALEMAN DE 15 DE DICIEMBRE DE 1983.**

#### **VI) PROTECCION JURIDICA DEL DERECHO A LA INTIMIDAD EN EL DERECHO ESPAÑOL.**

#### **VII) LA LEY ORGANICA 5/1992 DE 31 DE OCTUBRE DE 1992 SOBRE PROTECCION DE DATOS PERSONALES Y SU POSIBLE INCONSTITUCIONALIDAD.**

## D) La Figura del Defensor del Pueblo y la Protección de los Datos de Caracter Personal

De acuerdo con el art. 54 de la Constitución Española, el Defensor del Pueblo es el Alto Comisionado de las Cortes Generales designado por éstas para la defensa de los derechos y libertades fundamentales incluidas en el Título I de nuestra Carta Magna.

En el ejercicio de esta misión el Defensor del Pueblo está legitimado para fiscalizar o supervisar las actividades de la Administración<sup>1</sup>, dando cuenta a

■ 1 El art. 9.1 de la L.O.D.P. interpreta el concepto de la actividad de la Administración concretándolo en los actos administrativos y resoluciones de la Administración pública y sus agentes.

La supervisión de la Administración aparece pues, en el citado artículo 9.1, como la función específica del Defensor del Pueblo; supervisión que éste debe llevar a cabo "a la luz de lo dispuesto en el art. 103.1 CE y el respeto debido a los derechos proclamados en su Título I". Lo cual parece indicar que el respeto de los derechos del Título I es más bien un límite a la función que la función misma.

Ver con relación al origen, naturaleza y alcance de la figura del Defensor del Pueblo, entre otros, los trabajos:

-Antonio Bar

La regulación jurídica de los "defensores del pueblo regionales": ¿cooperación o conflicto?. Revista de Derecho político núms. 18-19, Verano Otoño 1983, 77.

-Marcos Carrillo López

El Defensor del Pueblo: ¿factor de democratización?. Revista Jurídica de Cataluña, núm. 4, 1980, 9.

-Alvaro Gil Robles

El Defensor del Pueblo (comentario en torno a una proposición de ley orgánica). Madrid, 1979. Civitas.

-Victor Fairén Guillén

Actividades recientes de algunos "ombudsmannen" (incluido el Defensor del Pueblo). Revista Española de Derecho Administrativo núm.46, Abril-Junio 1985, 227.

-Victor Fairén Guillén.

Normas y Notas sobre el "Ombudsman" de Finlandia. Revista de Administración Pública, núm. 93, Sep-Dic. 1960, 345.

-Victor Fairén Guillén.

Normas y notas sobre el "Ombudsman" de Suecia. Revista de Estudios Políticos, núm. 21, Mayo-Junio 1981, 127.

-Héctor Gros Espiell

El ombudsman. Su interés en la actual situación de Hispanoamérica. Revista de las Cortes Generales, núm. 4, Enero-Abril 1985, 199.

-Joaquín Varela Suanzes-Carpegna

La naturaleza jurídica del Defensor del Pueblo. Revista Española de Derecho Constitucional, nº 8, Mayo-Agosto 1983, 63.

las Cortes Generales. Inspirado en la Institución del Ombudsman (figura de origen sueco que ha sido imitada por todos los países con diversas denominaciones, Comisario, Mediateur, Proveedor de Justicia) está regulada por la Ley Orgánica 3/1981 de 6 de abril<sup>2</sup>.

De acuerdo con la Constitución, el Defensor del Pueblo está legitimado para presentar recurso de amparo o inconstitucionalidad ante el Tribunal Constitucional con el efecto de garantizar de la manera más eficaz el cumplimiento de su misión de defensa o tutela de los derechos y libertades ciudadanas.

El derecho de autodeterminación informativa, reconocido en el art. 18.4 de nuestro texto constitucional, se incardina dentro del Título I del mismo, correspondiendo por tanto, al Defensor del Pueblo la labor de supervisión o vigilancia de aquellos casos en que conozca se ha producido una violación o desconocimiento de este derecho o de las libertades que el mismo ampara.

-Antonio Vñas Otero

Del 'Tribunus Plebis' romano al Defensor del Pueblo. La Ley, 1984-3, 942.

Angela de la Cruz Mera

-El defensor del pueblo (I y II). Boletín de Información del M<sup>o</sup> de Justicia num. 1507-1508, 25 Octubre y 5 Noviembre, 1988.

- 2 La Ley 35/1985 de 6 de noviembre regula las relaciones entre el Defensor del Pueblo y las figuras similares que se han ido creando en distintas Comunidades Autónomas: Síndic de Greuges, Valedor del Pueblo, Diputado de la Comisión de Justicia. El Consejo de la Unión ha aprobado un proyecto del Parlamento Europeo sobre el estatuto y las condiciones generales del ejercicio de las funciones del Defensor del Pueblo europeo. Esa nueva figura que viene instituida en el Tratado de Maastricht (art. 138 F) estará capacitada para recibir las peticiones de cualquier ciudadano de la Unión. Todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su sede social en un Estado miembro de la Unión podrá acometer al Defensor del Pueblo, directamente o por mediación de un miembro del Parlamento Europeo, una reclamación relativa a un caso de mala administración en la actuación de las instituciones u órganos comunitarios, **con exclusión del Tribunal de Justicia y el Tribunal de Primera Instancia** en el ejercicio de sus funciones. El Defensor del Pueblo informará de la reclamación a la institución u órgano interesado tan pronto como la reciba.

El Defensor del Pueblo contribuirá a descubrir los casos de mala administración en la acción de las instituciones y órganos comunitarios, con exclusión del Tribunal de Justicia y del Tribunal de Primera Instancia en el ejercicio de sus funciones judiciales, y a formular recomendaciones para remediarlos.

El Defensor del Pueblo europeo deberá ejercer sus funciones con total independencia y durante su mandato no podrá desempeñar ninguna otra actividad profesional.

El Defensor del Pueblo procederá a todas las investigaciones que considere necesarias para aclarar todo posible caso de mala administración en la actuación de las instituciones y órganos comunitarios, bien por iniciativa propia, bien como consecuencia de una reclamación. Informará de ello a la institución u órgano afectado, que podrá comunicarle cualquier observación útil.

Ha habido una cierta polémica doctrinal a la hora de determinar con precisión la función que en nuestro Derecho tiene asignada el Defensor del Pueblo; en efecto, a la hora de interpretar el art. 54 de nuestro texto constitucional se ha planteado el problema de saber si la defensa de los derechos comprendidos en el Título I y la supervisión de la Administración, constituyen dos funciones distintas, autónomas, a realizar por el Defensor del Pueblo o se trata más bien de una única función, la defensa de los derechos del Título I, para lo cual, y con esa finalidad, el Defensor supervisa la actividad de la Administración.

Es, por consiguiente, necesario conocer con la mayor precisión posible la naturaleza y alcance de este nuevo derecho de la protección de los datos personales o, utilizando la terminología del Tribunal Constitucional alemán - aceptada ya por la mejor doctrina-, derecho a la autodeterminación informativa, sobre cuyo desarrollo el Defensor del Pueblo también deberá prestar, ya lo ha hecho de facto, su función de vigilancia o tutela.

Como es sabido, tanto en nuestro texto constitucional (art. 162.1.a) como la LOTC (art. 32.1.b) han legitimado al Defensor del Pueblo para el ejercicio del recurso de inconstitucionalidad sin establecer expresamente ningún tipo de condición o limitación al respecto. Precisamente sobre la Ley Orgánica 5/1992 que desarrolla el art. 14.4 de la Constitución el Defensor del Pueblo ha planteado recurso de inconstitucionalidad.

Así, por ejemplo, el Informe Anual del Defensor del Pueblo, presentado en el Congreso de los Diputados el 20 de abril de 1989, que en su capítulo V, relativo al Derecho a la Intimidad (art. 18 de la Constitución) señala que ... "el ciudadano de nuestros días cada vez está más integrado en las variadas bases de datos de la Administración y de entes privados" y afirma que "en nuestro país no existe aún una normativa adecuada que regule la utilización de todas estas bases de datos... Preocupa esta circunstancia al Defensor del Pueblo e incluso la posibilidad de que debido a esta carencia de regulación concreta, se permitan abusos o una utilización inadecuada, e incluso inconstitucional, de tales bases de datos. Se hace, pues, urgente dar cumplimiento a la previsión legal contenida en el artículo 18.4 de la Constitución Española".

Deben ser también subrayados los informes de 1990 y 1992. En el primero de ellos se señala la "especial importancia del control efectivo de tales bases de datos en lo que se refiere al ámbito jurídico, por cuanto en el de las Administraciones Públicas directamente y organismos o entes de ellos dependientes, está ya prevista la intervención del Defensor del Pueblo, y el Informe Anual de 1992, en que se aborda el tema de la utilización de los datos de carácter personal por las Fuerzas y Cuerpos de Seguridad del Estado cuanto estos datos obran en ficheros no automatizados o dimanen de filmaciones: se señala que si bien esta materia conoce de regulación específica la LO 5/1992 y la Ley 30/92 han llenado en parte el vacío legal, aunque no lo hacen de forma plena si constituyen un marco de referencia imprescindible. También se señala, en relación con el tratamiento de datos de carácter personal por empresas de seguridad privada, que tras la Ley 23/92 de 30 de julio, de Seguridad Privada, no tiene amparo legal el mantenimiento de bancos de datos o fichas con datos personales relativas a personas que hubieran sido intervenidas dentro de las funciones de protección que ejercen estos vigilantes.

## II) Naturaleza del Derecho de Protección de la Autodeterminación Informativa

Al sistema jurídico le corresponde actuar atento a las nuevas necesidades demandadas por una sociedad crecientemente informatizada, haciendo así también un ejercicio de adaptación interna de contenidos y valores.

Uno de los aspectos más importantes de la adaptación del Derecho a estas nuevas situaciones es el incipiente, pero firme, reconocimiento en los textos y en la jurisprudencia constitucional de un nuevo derecho fundamental, el derecho a la autodeterminación informativa<sup>3</sup>. Derecho incardinado dentro del ámbito de los derechos de la personalidad.

Se ha señalado con rotundidad que una sociedad desarrollada no puede ignorar que la informática aporta instrumentos insustituibles para recoger, almacenar, clasificar, racionalizar y transmitir los datos e informaciones necesarios para la gestión de toda clase de servicios y actividades.

Su progresiva e imparable implantación invade todas las esferas sociales afectando a las relaciones laborales, al ámbito de actuación de las entidades crediticias y financieras y al mundo de los medios de comunicación, llegando a romper las fronteras de la intimidad y saltando con asombrosa facilidad por encima de los límites tradicionalmente establecidos.

Por derechos de la personalidad debe entenderse el conjunto de aquellos que conceden un poder a las personas para proteger la esencia del ser humano y sus más importantes cualidades. Entre estos derechos se encuentra, pues, el Derecho a la intimidad personal recogido en el art. 18.1 de nuestra Constitución.

Cabe recordar que la construcción doctrinal de los derechos de la personalidad encuentra su origen en el ordenamiento jurídico privado, en donde por su consideración de innatos al ser humano, se les califica de intransmisibles, irrenunciables e imprescriptibles.

Algunos de estos derechos están expresamente consagrados en las Constituciones democráticas. Entre ellas, la Constitución española de 1978 reconoce

<sup>3</sup> A este tenor presenta un interés especial, a nuestro juicio, el estudio de Antonio Enrique Pérez-Luño sobre "Los Derechos Humanos en la Sociedad Tecnológica". Cuadernos y Debates (Libertad Informática y Leyes de Protección de Datos personales), publicado por el Centro de Estudios Constitucionales. Madrid, 1989.

Ver: "Los límites al derecho fundamental a la autodeterminación informativa en la Ley Española de Protección de Datos (LORTAD)", por Vicente López-Ibor Mayor. Actualidad Informática Aranzadi, nº 8, Julio 1993.

junto con el derecho a la libertad y a la seguridad personal (en sus diversas acepciones), el derecho al honor, a la intimidad personal y familiar y a la propia imagen (art. 18).

El derecho a la intimidad personal está directamente vinculado a la dignidad de la persona y, como señala el Tribunal Constitucional en su sentencia de 17 de octubre de 1.991, "implica la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario -según las pautas de nuestra cultura- para mantener una calidad mínima de la vida humana."<sup>4</sup>

En nuestros días una de las cuestiones más relevantes del derecho a la intimidad y de esa exigencia de calidad mínima de la vida humana, se centra en la información que sobre los ámbitos más reservados e íntimos de cada persona, pueda disponerse o utilizarse por terceros. La protección del Derecho se manifiesta en este caso a través del control del interesado en relación con el acceso de otros a la información más personal, a los datos más reservados de cada uno.<sup>5</sup>

De tal manera que el propio Tribunal Constitucional ha señalado, en la aludida Sentencia de 1991, como uno de los ámbitos protegidos de la intimidad personal, la "protección frente a nuestros datos personales,..." sobre todo si tenemos en cuenta el vertiginoso avance de las tecnologías de la información".

El derecho a la autodeterminación informativa se configura, pues, como un derecho fundamental de la persona humana, que entendemos consagrado constitucionalmente en nuestro texto fundamental en el artículo 18.4 cuando se establece "la necesidad de limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos".

No basta, sin embargo, la afirmación de la existencia de este nuevo derecho, que reconoce a la persona la facultad de control sobre su propia información -"la persona como dueño y señor de sus datos"- sino que es necesario además elaborar el contenido y delimitar el contorno constitucional del mismo. Para ello debemos valorar la respuesta ofrecida por otros ordenamientos de nuestro ámbito cultural y la más reciente jurisprudencia constitucional europea en relación a esta materia.

■ 4 STC 17 de octubre de 1991. Recurso de amparo nº 492/1989; ver también STC 231/1985 fundamento jurídico 3º.

■ 5 Ver el capítulo Derecho a la Intimidad: calidad y control de la infracción del trabajo de Vicente López-Ibor Mayor sobre "La legislación sobre informática en el ordenamiento jurídico español. Iº Congreso sobre Derecho Informático. Publicación de la Facultad de Derecho de la Universidad de Zaragoza. 1992.

Este derecho, hasta 1978, no había sido recogido de forma expresa en nuestros textos constitucionales. Igualmente ocurría en Derecho Comparado, donde las Constituciones no solían reconocer de forma expresa este derecho, el cual sí resultaba protegido a la luz del principio general de respeto a la dignidad de la persona humana. No obstante, la Constitución portuguesa de 1976 lo reconoce, como veremos, en su art. 33.

### III) La Protección de Datos Personales en el derecho Comparado, El Convenio del Consejo de Europa

La protección de datos personales en el Derecho Comparado ha tenido y tiene una triple proyección. En primer lugar, por la existencia de disposiciones legislativas que la regulan<sup>6</sup>, en segundo término por la ratificación del Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal<sup>7</sup>, y finalmente, por el desarrollo de una jurisprudencia constitucional favorable al reconocimiento de este nuevo derecho de la personalidad, el derecho a la autodeterminación informativa.

En Francia es de mencionar la Ley orgánica 78/17, de 1978, en la que se consagran principios, definiciones, derechos y obligaciones en el campo del tratamiento automatizado de los datos personales y su repercusión sobre las actividades públicas.

En los Estados Unidos cabe destacar la "Privacy Act" de 1974 y la "Data Protection Act" de 1984.

En USA en 1978 se publica el "Financial Institutions Regulatory Act" (A.R. 14275) que contiene las primeras normas sobre sistemas de transferencia electrónica del dinero y sobre la relativa tutela de la "privacy". Se exige al Instituto financiero encargado de efectuar la transferencia por medio del EFT

■ 6 A este respecto cabe destacar además de la emblemática Ley dictada por el Iard de Hesse el 7 de octubre de 1990, la ley sueca de 11 de mayo de 1977, la ley federal alemana de 27 de enero de 1977 (Bundesgesetzblatt 1-2-1977), la francesa de 6 de enero de 1978 y la inglesa de 12 de julio de 1984. Especial relevancia presenta el art. 35 de la Constitución portuguesa de 1976.

■ 7 En relación con la limitación del tratamiento automatizado de los datos, el Comité de Ministros del Consejo de Europa ha adoptado diversas Recomendaciones relativas a la protección de los datos personales en función de los fines que la utilización de estos datos persigue:

-En relación con actividades de Marketing: Recomendación nº R (85) 20 de 25 de octubre de 1985.

-Actividades relacionadas con la Seguridad Social: Recomendación nº R (86) de 23 de enero de 1986.

-En relación con las actividades policiales: Recomendación nº R (87) 15 de 17 de septiembre de 1987.

-En actividades relacionadas con el fomento del empleo: Recomendación nº R (89) 2 de 18 de enero de 1989.

-Respecto a la utilización de estos datos por los organismos públicos: Recomendación nº R (91) 10 de 9 de septiembre de 1991.



(Electronic Fund Transfers) informar al usuario de los derechos, responsabilidad y ventajas derivadas de tal uso, estudiar los métodos para prevenir abusos y errores, dar curso inmediatamente a una comprobación escrita de todas las transacciones, hacer extractados cálculos periódicos.

En Alemania la regulación más importante es la contenida en la Ley promulgada el 27 de enero de 1977, posteriormente derogada en favor de un nuevo texto que entró en vigor en 1991. El Derecho Alemán de Protección de Datos está inspirado en principios básicos derivados de la autodeterminación informativa. Ese Derecho fue confirmado por el Tribunal Federal Constitucional en 1983. De acuerdo con la máxima de la Federación Constitucional en 1983, el individuo es el dueño y señor de sus datos. En tanto, por interés general, por ejemplo como contribuyente, pueda ser obligado a proporcionarlos, las preguntas deben limitarse a lo estrictamente necesario. El uso de datos personales está en principio prohibido en la República Federal Alemana.

Existen regulaciones legales explícitas para las excepciones. Datos personales pueden ser recabados y usados sólo con una vinculación finalista claramente definida. El individuo tiene derecho a saber qué uso de sus datos hacen las instancias que los archivan. Todo ciudadano puede solicitar ayuda al Comisionado para la Protección de Datos, cuando sospecha un uso ilegal de sus datos. La protección de los datos es controlada por el Comisionado Federal y los Comisionados de los Lander. Estos controlan la observación de las leyes en parte por iniciativa propia y en parte por quejas de los ciudadanos.

Las características del cargo quedan claras tomando como ejemplo al Comisionado Federal. Este es elegido por el Parlamento Federal y posee por ello una legitimación democrática especial. Posee asimismo el derecho a negarse a dar testimonio ante los Tribunales, lo cual protege a todos los ciudadanos de eventuales desventajas derivadas de quejas. Informa al Parlamento acerca de sus actividades, realiza informes y peritajes y sugiere mejoras. Asimismo promueve la cooperación con los colegas en los Länder.

Además de las mencionadas hasta ahora, existen leyes que regulan la protección de los datos personales en Austria (Ley 18 octubre 1978, n° 565), Canadá (Privacy Act. 1982), Dinamarca (Ley 8 de junio de 1978, n° 293, sobre los registros privados y Ley 8 de junio de 1978, n° 294, sobre los registros de la Administración pública), Gran Bretaña (Ley 12 julio 1984)<sup>8</sup>, Islandia (Ley n°

<sup>8</sup> En 1960 William Prosser propone una sistematización del concepto de privacy, que hasta entonces se había desarrollado al hilo de los casos concretos, conforme a la tradición del Common Law. Prosser individualiza cuatro situaciones distintas de violación de la privacy protegidas por el Common Law vigente en los Estados Unidos:

\*1. intrusión en la soledad de la vida de una persona o en sus asuntos privados;

63, 1984), Israel (Ley 574 II-1981), Italia (Ley 1 abril 1981, n° 121: pública), Luxemburgo (Ley 30 marzo 1979: identificación numérica de las personas físicas y jurídicas, Ley 31 marzo: uso de los datos nominativos de los sistemas informáticos), Noruega (Ley 9 junio 1978, n° 48), Suecia (Ley 11 mayo 1973, n° 289, modificada por Ley 1 julio 1982: recogida de datos), Suiza (Directivas del Consejo Federal sobre el procesamiento de datos por los entes federales, 16 marzo 1981).

El Comité de Ministros del Consejo de Europa adoptó, en 1973 y 1974, *dos Resoluciones sobre la protección de la vida Privada de los individuos*, con respecto a los bancos de datos electrónicos: la primera para el sector privado Resolución (73) 22; y la segunda para el sector público (74) 29.

Los principales aspectos desprendidos de estas dos Resoluciones, pueden sintetizarse en los puntos siguientes:

-Las informaciones no deben ser recopiladas o tratadas según procedimientos desleales o ilícitos.

-*La exactitud de las informaciones a registrar y su puesta al día deben estar aseguradas.* (Seguridad y calidad de la información; Actualización de datos).

-*Deben precisarse los fines del registro de datos personales, para que sea posible verificar la adecuación de aquéllos a éstos.* Vigilando que las informaciones no sean utilizadas para aquello por lo que fueron solicitadas, sin que el tiempo de conservación de los mismos exceda de la permitido para alcanzar la citada finalidad. (La información personal dada para una finalidad determinada no puede ser utilizada para otra diferente, si no es con consentimiento del sujeto interesado).

-*Las informaciones sensibles no deben ser registradas salvo si se dan una serie de garantías particulares.* (Confidencialidad).

2. divulgación de hechos embarazosos que afectan a la persona;

3. publicidad que podría desprestigiar a la persona ante la opinión pública;

4. apropiación (con ventaja para la otra parte) del nombre o del aspecto físico del querellante\*.

La teoría de Prosser fue criticada porque hacía añicos el "general right to privacy" elaborado por Warren y Brandeis, provocando la crisis del concepto jurídico de privacy que, hasta ese momento, era considerado unitario.

Precisamente estas polémicas y las dudas que de él derivaron en la aplicación del concepto de privacy en los numerosos casos concretos demostraron que el problema era sentido en los Estados Unidos. La conclusión legislativa de este debate doctrinal se produjo con la incorporación del concepto de privacy en la United States Privacy Act\* de 1973.

*-La creación de los bancos de datos y su seguridad material deben ser transparentes.*

*-Toda persona tiene derecho a conocer las informaciones que le afecten, así como el derecho a rectificación de las mismas.*

En 1980, el Comité de Ministros del Consejo de Europa adoptó un nuevo convenio internacional para la protección de las personas respecto al tratamiento automatizado de los datos de carácter personal. Presentado este Convenio a la firma de los Estados miembros del Consejo de Europa el 28 de enero de 1981, entró en vigor el 1 de octubre de 1985.

El Convenio de 1981 establece unos principios básicos respecto a los datos de carácter personal objeto de tratamiento automatizado, y que se regulan en los artículos 5, 6 y 8 del mismo:

-Principios de lealtad y legalidad.

-Principio de proporcionalidad respecto a su finalidad.

-Principio de exactitud.

-Principio de seguridad.

-Principio de protección especial de los datos sensibles.

-Principio de acceso a los ficheros automatizados y a los datos personales, que se extiende al derecho a la publicidad de los ficheros, al conocimiento de los datos que afectan al individuo, a la rectificación de esos datos y a un recurso si no se ha obtenido la pretensión planteada de acuerdo con las garantías anteriores.

Así pues el Convenio del Consejo de Europa recoge tanto el conjunto de derechos de carácter activo, como el derecho al consentimiento previo a la captación de los datos personales de cada uno -art. 6-; a la información sobre la recogida de datos que afectan a la propia persona -art. 7-; al acceso de los datos recogidos en una base ya creada -art. 14-; a la rectificación o cancelación del contenido de una base en uso -art. 15-; a la impugnación o recurso frente a la negativa a ejercitar las facultades descritas -art. 17-; junto con los tradicionales derechos de contenido negativo, como por ejemplo, la interdicción del tratamiento automatizado de los datos de carácter personal que revelen la ideología, religión o creencias -art. 7-.

## IV) Derecho Comunitario y Protección de Datos

Las instituciones de la Comunidad Europea son conscientes de la necesidad de establecer unos umbrales de protección para salvaguardar los derechos de la persona frente al progreso técnico de la informática sin obstaculizar con ello el desarrollo de la industria europea de la informática en el flujo transfronterizo de los datos almacenados en memoria.

Los fundamentos jurídicos que justifican la intervención legislativa de la Comunidad en este campo son:

- El art. 100 del TCE, relativo a la aproximación de las legislaciones nacionales que incidan directamente en el establecimiento o el funcionamiento del Mercado Común.

- El art. 235 TCE, que autoriza al Consejo a adoptar las disposiciones pertinentes cuando resulte necesaria una acción de la Comunidad para lograr uno de los objetivos de la Comunidad sin que el Tratado contenga disposiciones explícitas al respecto.

- El Preámbulo del Acta Única en el que sus signatarios se comprometen a promover la democracia basándose en los derechos fundamentales.

El Parlamento Europeo fue la primera institución de la Comunidad que llamó la atención de las demás instancias comunitarias y nacionales, así como de la opinión pública, sobre los peligros que para la intimidad del ciudadano puede representar la informática. Así el 21 de febrero de 1975 aprobó el Parlamento Europeo su primera resolución en esta materia<sup>9</sup>. En dicha resolución pedía a la Comisión que elaborase una directiva con el objeto de proteger a los ciudadanos de los Estados Miembros de la CE contra los abusos a que puede dar lugar el tratamiento informático de datos personales, tanto en el sector privado como público. El PE proponía como base de trabajo para la Comisión una investigación que efectuaría la Comisión de Asuntos Jurídicos del PE. Dicha investigación no se efectuó hasta 1978. El 8 de mayo de 1979 el PE adoptó otra resolución<sup>10</sup> en la que reiteraba su petición a la Comisión. Sin embargo la Comisión consideró en aquel momento no proponer al Consejo la adopción de regulación alguna puesto que estimaba que era preferible esperar a la conclusión de los trabajos que en aquel momento se estaban desarrollando en el

■ 9 DO C 80/75.

■ 10 DO C 140/79.

Consejo de Europa y que culminarían con la adopción del Convenio de 1981. El 29 de julio de 1981 la Comisión adoptó una Recomendación<sup>11</sup> en la que pedía a los Estados Miembros que ratificasen cuanto antes este Convenio. Tras la apertura a la firma del Convenio de 1981, el PE volvió a adoptar otra resolución el 9 de marzo de 1982<sup>12</sup> en la que puso de manifiesto sus dudas en relación con la rápida entrada en vigor del Convenio, e insistió en la preparación de una directiva comunitaria por un lado, y por otro señaló que esperaba que la Comunidad, como tal, se adhiriera al Convenio del Consejo de Europa. El PE continuó manifestando su preocupación al respecto e insistiendo a la Comisión para que actuara a nivel comunitario en otras dos resoluciones de 26 de marzo de 1984<sup>13</sup>. Conviene señalar que todos los Estados Miembros de la Comunidad firmaron en su momento el Convenio del Consejo de Europa. Dinamarca, Francia, Alemania, Irlanda, Luxemburgo, el Reino Unido, y España son los Estados Miembros que lo han ratificado hasta el momento.<sup>14</sup>

Finalmente la Comisión presentó al Consejo las siguientes propuestas legislativas:

- Una propuesta de directiva relativa a la protección de las personas en lo que se refiere al tratamiento de datos personales<sup>15</sup>, a la que nos referiremos a continuación.

- Una propuesta de directiva relativa a la protección de los datos personales y de la intimidad en relación con las redes públicas digitales de telecomunicación y, en particular, la red digital de servicios integrados (RDSI) y las redes móviles digitales públicas<sup>16</sup>.

- Una propuesta de decisión en el ámbito de la seguridad de los sistemas de información.<sup>17</sup>

- Una propuesta de reglamento relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico<sup>18</sup>.

▪ 11 DO L 246/81.

▪ 12 DO C 87/92.

▪ 13 DO C 117/84.

▪ 14 Los datos que aquí se recogen han sido tomados de las *Fichas técnicas sobre el Parlamento Europeo y las actividades de la Comunidad Europea*, Parlamento Europeo, Dirección General de Estudios (1983), y de las *Fichas técnicas sobre el Parlamento Europeo y las actividades de la Unión Europea*, Parlamento Europeo, Dirección General de Estudios (1994).

▪ 15 DO C 277/90.

▪ 16 DO C 277/90.

▪ 17 DO C 277/90.

▪ 18 DO C 291/89.

Hasta ahora han sido aprobados por el Consejo la propuesta de decisión relativa a la seguridad de los sistemas de información<sup>19</sup> y la propuesta de reglamento relativo a la transmisión de informaciones estadísticas<sup>20</sup>.

A continuación se examina el contenido y significación de la Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, cuyo fin es armonizar e integrar las normativas nacionales existentes en la materia, extendiendo las garantías necesarias a todo el territorio de la Comunidad.

### **1. La propuesta modificada de Directiva del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos Personales y la libre circulación de estos datos.**<sup>21</sup>

#### *a) Finalidad de la Propuesta*

Esta Propuesta responde a la doble necesidad de facilitar y fomentar la libre circulación de los datos personales, garantizando al mismo tiempo la estricta protección de la intimidad de las personas. Encuentra su justificación en el Convenio 108 del Consejo de Europa de 28 de enero de 1981, relativa a la protección de las personas en lo referente al tratamiento automatizado de los datos personales.

En este sentido, los datos personales a los que se aplique un tratamiento automatizado deberán ser:

- Objetivos y tratados legal y lícitamente.

■ 19 DO L 132/92.

■ 20 DO L 151/90.

■ 21 El Comité Económico y Social emitió Dictamen (DOCE N° C 159/93 de 17.6.91) sobre esta Propuesta, señalando:

-La falta de legislación de este tipo en cinco Estados miembros (pese a la existencia del art. 8 del Convenio para la Protección de los Derechos Humanos) es la principal preocupación.

-Por otra parte, la libre circulación de las personas debería exigir un mínimo de conformidad entre los Estados miembros en lo relativo a las obligaciones que atañen a los organismos que realizan tratamientos de informaciones nominativas, así como en lo relativo a los derechos de las personas y sus modalidades de ejercicio.

-Además, se observa, y no deja de ser sorprendente, que las exigencias de cara al sector privado podrán resultar superiores a las que se imponen al sector público (posibles exigencias de información para la comunicación de datos por el sector privado; ausencia de dichas exigencias para la comunicación de datos entre autoridades públicas). En materia de derecho de las personas, no está establecida la coherencia entre un determinado número de disposiciones generales o particulares.

-No obstante, hay que dejar bien claro que la finalidad de esta protección es garantizar, en el territorio de cada Estado miembro, el respeto de los derechos y libertades fundamentales de toda persona física, cualquiera que sean su nacionalidad o su residencia, así como, en concreto, el respeto de su derecho a la intimidad cuando se trate del tratamiento automatizado de los datos personales que le afecten.

- Registrados con fines determinados y legítimos y no utilizados de modo incompatible con dichos fines.

- Adecuados, pertinentes y no excesivos en relación con los fines para los que han sido registrados.

- Exactos y si fuere necesario actualizados.

- Conservados de tal modo que permitan la identificación de las personas interesadas durante un período que no exceda del necesario según los fines para los que fueron registrados.

Salvo que el derecho interno no disponga de unas garantías apropiadas, no podrán tratarse automáticamente los datos personales que revelen el origen racial, opiniones políticas, convicciones religiosas o de otro tipo.

Como garantía de protección de la intimidad personal, esta Propuesta reconoce asimismo al interesado los siguientes poderes:

-conocer la existencia de un fichero automatizado de datos personales, sus fines principales, así como la identidad y residencia habitual o el establecimiento principal del responsable del fichero;

-obtener a intervalos razonables y sin plazos o gastos excesivos, la confirmación de la existencia o no en el fichero automatizado de datos personales que le afecten, así como la comunicación de los mismos de forma inteligible;

-obtener, si hubiera lugar, la rectificación de dichos datos o su anulación si hubieran sido tratados violando aquellas disposiciones del derecho interno que hacen efectivos los principios básicos que figuran en los artículos 5 y 6 del Convenio;

-disponer de un recurso si no se da curso a una solicitud de confirmación o, en su caso, de comunicación, rectificación o anulación, tal y como se indica en los apartados b y c del artículo 8 del Convenio.

Así pues, toda persona que ordene o efectúe un tratamiento de informaciones nominativas se compromete por tanto, de cara a las personas interesadas, a tomar las precauciones necesarias para preservar la seguridad de las informaciones, y en especial, impedir que sean deformadas, dañadas o comunicadas a terceros no autorizados.



Finalmente, y con el fin de garantizar la libre circulación de las personas, es conveniente exigir un mínimo de uniformidad entre los Estados miembros en lo relativo a las obligaciones que atañen a los organismos que realizan tratamientos de informaciones nominativas, así como en lo relativo a los derechos de las personas y sus modalidades de ejercicio.

#### *b) Novedades de la Propuesta*

Las principales novedades que ofrece esta Propuesta respecto de la anterior, la cual fue presentada a la Comisión el pasado 27 de julio de 1990 junto con la Propuesta de Directiva relativa a la protección de los datos personales y la intimidad en relación con las redes públicas digitales de telecomunicación, y en particular la Red Digital de Servicios Integrados, y junto a una Propuesta de Decisión en el ámbito de la seguridad de la información, se refieren a los siguientes aspectos:

##### *bl.) Concepción de la protección.*

En primer lugar trata de eliminar las diferencias de protección entre el sector público y privado.

En segundo lugar, evitar el riesgo de burocratización en los métodos empleados para garantizar dicha protección, mediante el establecimiento de reglas claras y sencillas relativas a los procedimientos de notificación a la autoridad de control, así como en relación a los códigos de conducta.

##### *b2.) Conceptos y definiciones.*

Por un lado se ha actualizado el concepto de "fichero"<sup>22</sup> del artículo 2, a la luz del desarrollo de la automatización y de las telecomunicaciones, así como la definición de "tratamiento de datos personales"<sup>23</sup> mediante la inclusión de la actividad de recogida de datos.

■ 22 Se ofrece esta definición, que comprende tanto los ficheros automatizados como los no automatizados. Permite, en lo referente a los tratamientos de datos no automatizados, circunscribir el ámbito de aplicación de la Directiva a los datos estructurados para facilitar el acceso y la búsqueda de aquéllos que se refieran a personas físicas. De esta manera quedan excluidos los datos personales que no están organizados para su utilización en relación con los interesados. De hecho, estos datos no comportan los mismos riesgos para las personas y resulta más realista no someterlos a las mismas obligaciones. Para garantizar la protección de las personas, se precisa que los criterios de acceso deben tener "como objeto o efecto" facilitar la utilización o el cotejo de datos, para no obligar al interesado a revelar sus intenciones, lo que volvería muy delicada la aplicación de la normativa nacional.

Por último, se da preferencia al concepto de "cotejo" frente al de "interconexión", ya que puede aplicarse tanto a los tratamientos automatizados como a los ficheros de papel.

■ 23 La definición escogida también propugna un ámbito de aplicación amplio, que le permita garantizar la protección de las personas (enmienda 15), puesto que comprende los datos desde su recogida hasta su supresión, pasando por su organi-



Por otro lado se ha añadido una definición de los terceros a quienes se comunican datos personales, los cuales podrán ser tanto personas físicas como jurídicas (art. 2 f).

*b3.) Ambito de aplicaciones y exenciones especiales.*

Afecta fundamentalmente a tres ámbitos diferentes:

a) Tratamientos realizados por asociación sin ánimo de lucro: Se incluyen dentro del ámbito de aplicación de la Directiva, no obstante, se prevé la exención particular a la obligación de notificación al titular de los datos necesaria para garantizar la libertad de opinión.

b) Tratamiento con fines periodísticos: Se establece la "obligación" de que los Estados concedan las exenciones necesarias para conciliar la protección de la intimidad de los interesados con la libertad de expresión.

c) Tratamientos que responden a obligaciones de tipo jurídico: Se exoneran estos casos de la obligación de notificación.

*b4.) Terceros países.*

En relación con la posibilidad de transferencia de datos a terceros países, se establece la prohibición de efectuar dichas transferencias a países que no garanticen suficientemente el grado de protección. A estos efectos se establecen criterios de evaluación de la idoneidad de la protección.

Otra novedad importante que introduce la Propuesta es su nueva reestructuración, con el fin de hacer efectiva la supresión de la distinción formal entre sector público y sector privado, destacando en última instancia los diferentes elementos del mecanismo de protección.

## **2. El Acuerdo de SCHENGEN**

En el contexto europeo es importante también subrayar la creación de un Sistema Informático Schengen (SIS) derivado del Acuerdo del mismo nombre. El Convenio Schengen fue firmado el 14 de junio de 1985 por cinco Estados (Francia, República Federal Alemana, y los Países del BENELUX).

-zación, explotación, consulta, comunicación (por transmisión), difusión o cualquier forma de cesión (enmienda 16), interconexión y bloqueo.

Este Acuerdo tiene por objeto suprimir progresivamente los controles en las fronteras comunes, instaurando así un régimen de libre circulación para todos los ciudadanos pertenecientes a los Estados signatarios del Convenio.

El 27 de noviembre de 1990 Italia se adhiere a los cinco Estados mencionados. A continuación se incorporan España y Portugal el 18 de noviembre de 1991. Grecia es el décimo país signatario del Acuerdo en el mes de noviembre de 1992.

Una Convención suplementaria fue firmada en 1990 por los Estados fundadores, definiendo las condiciones de aplicación y las garantías de puesta en práctica de esta libre circulación. Esta Convención, estructurada a través de 152 artículos, modificó las Leyes nacionales sobre esta materia, y está sujeta a ratificación parlamentaria.

El Convenio de Schengen es un Convenio intergubernamental y no comunitario, y su firma en todos los Estados se va desarrollando en algunos casos por falta de seguridad, tanto en lo relativo al tráfico de personas como en función del control de drogas en las fronteras exteriores.

Este Convenio recoge también la cooperación policial en bases de datos nacionales conectadas por medio de un sistema central que se encuentra hoy en La Haya, dependientes del Ministerio holandés de Interior.

## **2.1. El Sistema de Información Schengen**

Los ficheros del Sistema de Información Schengen (S.I.S.), sistema que operará en todos los Estados miembros de Schengen y que cuenta con una oficina en Estrasburgo con funciones de apoyo técnico, contendrán más de ochocientas mil referencias, tanto personales como de otra índole. En el Convenio de aplicación del acuerdo Schengen de 19 de junio de 1990 se regula la protección de los datos de carácter personal para su tratamiento automatizado en el Título VI.

El S.I.S., tal como se regula en los arts. 92 a 130 del Convenio de Aplicación del Acuerdo Schengen, es un mecanismo de información común y de "libre circulación de datos" entre las Partes Contratantes de gran complejidad, y plantea numerosos problemas en relación con el respeto al derecho al honor y a la intimidad. No obstante, por motivos de la extensión de este trabajo, nos limitaremos a señalar brevemente algunos de ellos, y en especial los que se pueden relacionar con los preceptos de la Ley Orgánica 5/1992 de Regulación de Tratamiento Automatizado de Datos, en lo sucesivo LORTAD, que han

sido objeto de recurso de inconstitucionalidad interpuesto ante el Alto Tribunal por el Defensor del Pueblo.

El art. 93 del Convenio de aplicación del Acuerdo de Schengen señala que el objetivo del S.I.S. es preservar el orden y la seguridad pública, y hacer viable la aplicación del convenio en lo relativo a la libre circulación de personas por el territorio de los Estados firmantes, sirviéndose para este fin de la información que proporciona el sistema.

Mediante éste se puede acceder a los datos en él integrados y consultarlos directamente. El uso del S.I.S. está reservado a las comisarías y consulados. Cada Estado ha de comunicar al Comité ejecutivo la lista de las autoridades competentes autorizadas para acceder a los datos, especificando qué tipos de datos y con qué objeto pueden consultarlos.

En la Base de Datos constará entre otro tipo de información la referente a:

- Personas buscadas a efecto de extradición.
- Personas desaparecidas.
- Personas extranjeras incluidas en las "listas de no admisibles".
- Personas en interés de su propia protección o para prevenir amenazas.
- Testigos.

De acuerdo con el art. 94.3, respecto a las personas los elementos introducidos serán como máximos los siguientes:

- a. El nombre, los apellidos y en su caso los alias;
- b. los rasgos físicos;
- c. la primera letra del segundo nombre;
- d. fecha y lugar de nacimiento;
- e. el sexo;
- f. la nacionalidad;

- g. la indicación de que la persona de que se trate está armada;
- h. la indicación de que las personas de que se traten son violentas;
- i. el motivo de la inscripción;
- j. la conducta que debe observarse;

No se autorizarán otras anotaciones, mencionándose en particular la de los datos sensibles enumerados en el art. 6 del Convenio de 1981.

El Sistema de Información se integra por los siguientes componentes:

a) Sistema Central (C-SIS): realiza la función técnica de apoyo, asegurando la identidad permanente de las bases de datos nacionales, y distribuyendo en línea toda la información que se maneja en el espacio Schengen. La oficina está situada en Estrasburgo.

b) Sistema Nacional (N-SIS): realiza las funciones que se le asigna en cada país. Recopila información en cada Estado y la manda al Sistema Central, y recibe la que el Sistema Central a su vez le suministra del resto del espacio Schengen.

c) SIRENE: es el sistema suplementario de peticiones y consultas de ámbito nacional. A través de este mecanismo se van a producir importantes trasvases de información en el espacio Schengen.

EL Convenio exige que cada país parte en el Acuerdo cuente con una ley de protección de datos personales, y que vigile el cumplimiento de la ley y de sus garantías. En el Acuerdo de Adhesión del Reino de España, firmado en Bonn el 25 de junio de 1991, España se obligó a adoptar, antes de la ratificación del Acuerdo, con el fin de dar plena aplicación a las disposiciones del Convenio relativas al S.I.S., todas las iniciativas necesarias para que la legislación española fuera completada de conformidad con el Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con relación al tratamiento informatizado de datos de carácter personal, y con observancia de la recomendación R (87) 15, de 17 de septiembre de 1987 del Comité de Ministros del Consejo de Europa tendente a reglamentar la utilización de los datos de carácter personal en el sector policial. El cumplimiento de esta exigencia fue pues una de las causas que hizo que el legislador español regulará finalmente esta materia en 1992.

Conviene subrayar a este respecto que España, al ratificar el 31 de enero de 1984 el Convenio del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter temporal, ya se había obligado, de acuerdo con el art. 4 de este Convenio, a tomar en su derecho interno, las medidas necesarias para que fueran efectivos los principios que éste consagra. Estas medidas deberán haber sido tomadas, de acuerdo con el párrafo segundo de dicho artículo, a más tardar en el momento de su entrada en vigor, es decir, antes del 1 de octubre de 1985. Por lo tanto, España deberá haber desarrollado el precepto constitucional del art. 18.4 antes de dicha fecha para haber superado el carácter fragmentario y deficitario con que regulaba el tema en el Derecho español. El legislador fue sin embargo mucho más "eficiente" en el cumplimiento de la obligación, en principio de igual contenido, impuesta por el Convenio de aplicación de Schengen.

El propio Convenio del Consejo de Europa de 1981 partía de la necesidad de proteger y armonizar dos valores de distinta naturaleza: se pretendía encontrar una fórmula que garantizará por un lado la eliminación de controles que pudieran poner trabas a la libre circulación de la información "que constituye un principio fundamental, tanto para los individuos como para los pueblos"<sup>24</sup>, y encontrar al mismo tiempo asegurar la protección de datos a escala internacional. Como señala en su apartado 19 la memoria explicativa del convenio.

"El punto de partida del convenio estriba en que determinados derechos de la persona deben ser protegidos en relación con la libertad de circulación de la información sin consideración de fronteras."<sup>25</sup>

Se puede afirmar, evaluando este convenio, que el objetivo prevalente es el de la protección del derecho a la intimidad, sobre el otro interés, también de gran importancia, de la libre circulación de datos. Sin embargo, es obvio que en el Convenio de aplicación del Acuerdo de Schengen, el objetivo prioritario del S.I.S., es conseguir la mayor fluidez posible en la transmisión interfronteriza de datos, y la integración de un sistema de datos internacional, y que la protección de los datos de carácter personal es no un objetivo sino un mero instrumento de control de este sistema, lo que se va a reflejar en los problemas que en relación con la protección del derecho a la intimidad se plantean.

El art. 109 del Convenio de aplicación del Acuerdo Schengen establece que el derecho de toda persona a acceder a los datos que se refieran a ella y

■ 24 Memoria explicativa del Convenio 108 del Consejo de Europa, de 28 de enero de 1981, de protección de las personas en relación con el tratamiento automatizado de datos de carácter personal, apartado 9.

■ 25 *ibid.*

estén introducidos en el S.I.S. se ejercerá respetando el Derecho de la Parte Contratante ante la que se hubiera alegado tal derecho. Continúa este artículo diciendo:

“Si el Derecho nacional así lo prevé, la autoridad de control prevista en el apartado 1 del art. 114 decidirá si se facilita información y con arreglo a qué modalidades. Una Parte Contratante que no haya realizado la descripción no podrá facilitar información relativa a dichos datos, a no ser que previamente hubiera dado a la Parte Contratante informadora la ocasión de adoptar una posición”.

El párrafo segundo de este artículo dispone que **no se facilitará información a la persona de que se trate si dicha información pudiera ser perjudicial para la ejecución de la tarea legal consignada en la descripción o para la protección de los derechos y libertades de terceros. Se denegará en todos los casos durante el período de descripción con vistas a una vigilancia discreta.**

Esta limitación al derecho de acceso a los datos excede los presupuestos de excepción a este derecho que establece el art. 9 del Convenio de 1981, como también ocurre con el art. 22.2 de la LORTAD, que es uno de los preceptos recurrido como inconstitucional por el Defensor del Pueblo, por no respetar el contenido esencial del derecho a la intimidad. Hay que tener en cuenta que el S.I.S. no será únicamente utilizado por Fuerzas y Cuerpos de Seguridad<sup>26</sup>, sino también por consulados, y funcionarios de aduanas.

En relación con el derecho de información en la recogida de datos, el Convenio de aplicación del Acuerdo de Schengen no lo recoge expresamente. Sin embargo el art. 104 dispone:

1. El Derecho nacional de la Parte Contratante informadora se aplicará a la descripción, salvo que existan condiciones mas exigentes en el presente Convenio.

2. Siempre que el presente Convenio no establezca disposiciones particulares, se aplicará el Derecho de cada Parte Contratante a los datos introducidos en la parte nacional del S.I.S.

■ 26 En el art. 21 de la LORTAD se prevén excepciones extraordinarias al derecho de acceso a ficheros de las Fuerzas Armadas y Cuerpos de Seguridad que están justificadas por motivos de defensa del Estado o de la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que realizan. Estas excepciones estarían dentro de los límites previstos por el art. 9 del Convenio de 1981, y de las pautas marcadas por la Recomendación nº R (87) 15 adoptada por el Comité de Ministros del Consejo de Europa en 1987 sobre la reglamentación de la utilización de datos de carácter personal en el sector de la policía.

Sin embargo, la disposición española que regula el derecho de información en la recogida de datos ha sido sometida en el art. 22.1 de la LORTAD a excepciones de dudosa constitucionalidad como pone de manifiesto el recurso de inconstitucionalidad del Defensor del Pueblo que analizaremos posteriormente.

El art. 110 del Convenio de aplicación del Acuerdo de Schengen establece que toda persona podrá rectificar datos que contengan errores de hecho que se refieran a ella o hacer suprimir datos que contengan errores de derecho que se refieran a ella. Lo cual, obviamente nunca será posible en aquellos casos en que según el artículo anterior se puede denegar el acceso a los datos. Dado que el derecho de acceso a los ficheros es presupuesto necesario para el ejercicio de estos otros dos derechos, de ahí la importancia de las excepciones con que se restringe este.

El Convenio también plantea importantes problemas en relación con la cesión de datos y el derecho de los individuos a que ésta se haga con su consentimiento, excepto en casos excepcionales y tasados. El art. 19.1 de la LORTAD, cuyo objeto es también la regulación de la cesión de datos, ha sido otro de los preceptos cuya inconstitucionalidad denuncia el Defensor del Pueblo por no establecer la norma española las debidas garantías legales para proteger el contenido esencial del derecho a la intimidad.

Entre las disposiciones problemáticas del Convenio de aplicación del Acuerdo Schengen en esta materia resaltaremos lo establecido en el art. 107 que dispone:

“Cuando una persona ya haya sido objeto de descripción en el S.I.S., la Parte Contratante que introduzca una nueva descripción se pondrá de acuerdo con la Parte Contratante que hubiera introducido la primera descripción acerca de la integración de las descripciones. A tal fin, las Partes”.

La realización de esta integración de información, se hará, por consiguiente si ninguna consideración hacia la persona del afectado.

El Convenio prevé el ejercicio de acciones, en el territorio de la Parte Contratante, ante órgano jurisdiccional o la “autoridad competente en virtud del Derecho nacional”, a efectos de rectificación, supresión, información o indemnizaciones motivadas por una descripción que se refiera a ella.

Son muchas las críticas que se han hecho del Acuerdo Schengen en relación con temas como las consecuencias del Acuerdo para los refugiados y los



emigrantes de terceros Estados, y la puesta en manos de la policía de competencias no sometidas a control. Además, el Acuerdo pone en serio peligro el derecho a la defensa y el derecho a la intimidad, no respetando los estándares mínimos de protección de las personas, con respecto al tratamiento de datos de carácter personal, establecidos en el Convenio del Consejo de Europa de 1981.

El S.I.S. no ha entrado aún en funcionamiento debido principalmente a motivos de carácter técnico.

## V) La Sentencia del Tribunal Constitucional Alemán de 15 de Diciembre de 1983

Por su importancia y repercusión la Sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983 marca un hito fundamental en la afirmación constitucional del derecho a la autodeterminación informativa.

Esta Sentencia del Tribunal Federal Constitucional alemán subraya con claridad: *“Quien no sabe con suficiente seguridad qué datos relativos a su persona son conocidos en ciertos sectores de su entorno y no puede estimar aproximadamente qué conocimiento posee su interlocutor, puede verse limitado esencialmente en su libertad de planear y decidir con autodeterminación. Un orden social y un orden legal en el que los ciudadanos no saben quién sabe qué cosa y en qué circunstancias sobre ellos no es compatible con el derecho a la autodeterminación informativa (...). De ello se deriva que: el libre desarrollo de la personalidad presupone, bajo las condiciones del moderno tratamiento de datos, la protección del individuo de la obtención, el archivo, la utilización y la transferencia de sus datos personales sin límites (...). El derecho fundamental (del desarrollo de la personalidad) garantiza la potestad del individuo de determinar él mismo acerca de la cesión y el uso de sus datos personales (...). El individuo no tiene el derecho de dominio absoluto e ilimitado de “sus” datos (...). En principio, el individuo debe aceptar limitaciones de su derecho a la autodeterminación informativa en función de intereses generales predominantes”.*

El hecho central es, pues, la vinculación del desarrollo de la libre personalidad con el derecho de autodeterminación individual, al comprender éste la capacidad del individuo para afirmar su personalidad conociendo quién, qué, cuánto y con qué finalidad se conocen datos relativos a su persona.

En la citada sentencia de 15 de diciembre de 1983, en las condiciones de la elaboración moderna de datos, la protección del individuo contra la recogida, almacenamiento, utilización y difusión de sus datos personales queda englobado el derecho general de protección de la persona, de su dignidad. Este derecho



garantiza la facultad del individuo de determinar fundamentalmente por sí mismo la divulgación y la utilización de los datos referentes a su persona.

Por eso, el Tribunal alemán señaló que las limitaciones que pudieran establecerse a ese derecho a la "autodeterminación informativa" sólo eran admisibles en el marco de un *interés general superior* y necesitaban un fundamento legal basado en la Constitución, que debe responder al imperativo de *claridad normativa* inherente al Estado de Derecho. En su regulación debe el legislador observar, además, el principio de *proporcionalidad* y tiene que adoptar precauciones de índole organizativa y de derecho procesal susceptibles de contrarrestar el peligro de vulneración del *derecho de salvaguardia de la personalidad*.

## VI) Protección Jurídica del derecho a la Intimidad en el Derecho Español

El primer texto legislativo español posterior a la Constitución que protege de manera unitaria los derechos de la vida privada, es la *Ley 62/1978 de 26 de diciembre, de protección jurisdiccional de los derechos fundamentales de la persona*. Ulteriormente, fue aprobada la *Ley Orgánica 1/1982 de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y a la propia imagen*.

Según el Tribunal Constitucional, en la sentencia de 12 de noviembre de 1990, el criterio para determinar la legitimidad o ilegitimidad de las intromisiones en la intimidad de las personas, no es el de la veracidad, sino exclusivamente el de la *relevancia Pública del hecho divulgado*; es decir, que su comunicación a la opinión pública, aun siendo verdadera, resulte ser necesaria en función del interés público del asunto sobre el que se informa. Otra cosa muy diferente será el criterio empleado en la comprobación de esa relevancia pública o privada de la información en cuestión.

Según la *Ley Orgánica de 5 de mayo de 1982 (art. 7)*, tendrán consideración de *intromisiones ilegítimas en el ámbito de la protección de la intimidad* las siguientes actividades:

1. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.

2. La utilización de aparatos de escucha, dispositivos ópticos o de cualquier otro medio para el conocimiento de la vida íntima de las personas o

de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción.

3. La divulgación de hechos relativos a la vida privada de una persona o familia, que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.

4. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.

5. La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el art. 8.2.

6. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.

7. La divulgación de expresiones o hechos concernientes a una persona cuando la difame o la haga desmerecer en la consideración ajena.

En contra de lo que en principio pudiera parecer, este derecho fundamental no se configura como un obstáculo al desarrollo de la innovación informática, sino como el reconocimiento de un haz de facultades que permitan al ciudadano la garantía de su honor e intimidad personal y familiar, y el pleno y libre desarrollo de su personalidad.

Se trata, por tanto, no sólo de la posibilidad de impedir, en determinados casos, la captación de datos que pudieran afectar al núcleo más íntimo de cada ser humano; sino igualmente, de poder ejercitar aquellas acciones necesarias para poder asegurar la veracidad y exactitud de la información que sobre uno mismo disponen o están en condiciones de disponer o revelar los demás.

Como ha señalado Vittorio Frosini, el derecho a la intimidad es el derecho a proteger los datos que pertenecen al individuo, que se refieren a sus características personales almacenadas en las bases de datos gestionadas por terceros dentro del sector público o privado, o compuestas por información confidencial almacenada por la persona en una memoria artificial (electrónico) en vez de su propia memoria orgánica. Por consiguiente, este derecho ha

obtenido un sentido positivo, se ha convertido en el derecho a distribuir de forma razonable la información sobre uno mismo<sup>27</sup>.

## VII) La Ley Orgánica 5/1992 de 31 de Octubre de 1992 sobre Protección de Datos Personales y su posible Inconstitucionalidad.<sup>28</sup>

La Ley Orgánica 5/1992, publicada en el Boletín Oficial del Estado de 31 de octubre de 1992, desarrolla el artículo 18.4 de la Constitución Española, que dice:

*"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"*

Con notable retraso, el Legislador español decidió finalmente desarrollar el mandato constitucional del art. 18.4, así como la obligación adquirida por la ratificación en 1984 del Convenio de Protección de Datos Personales y el Consejo de Europa, de establecer de esta forma el adecuado ámbito jurídico y garantía de las libertades en relación con el uso de la Informática.

Sin embargo, esta Ley Orgánica contiene en su articulado elementos que ha merecido entre otras Instituciones del Defensor del Pueblo, una valoración jurídica de inconstitucionalidad trayendo consigo, consecuentemente, la presentación del correspondiente recurso del Alto órgano jurisdiccional.

El Defensor del Pueblo ha argumentado, a su juicio, la inconstitucionalidad del art. 19.1 de la Ley Orgánica, por entender que no se respeta el princi-

■ 27 Vittorio Frosini: Las implicaciones sociales de la revolución informática: sus ventajas e inconvenientes. pág. 7. nº 2. Enero 1990.

Ver también, entre otros:

- "Human rights in the computer age", del mismo autor (V. Frosini). Revista Informática e Direito. Junio-Abril 1989.

- "L'informatique au service du juriste", de Henri Manzanaras y Philippe Nectoux. Litec, Librairies Techniques, 1987.

■ 28 Ver, entre otros, los trabajos publicados en las Actas de III Congreso Iberoamericano de Informática y Derecho (Editorial Aranzadi, 1994).

- Notas acerca del Derecho de acceso recogido en el proyecto de Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal. Guillermo Orozco Pardo.

- La protección de datos personales en España: Presente y Futuro. Antonio E. Pérez Luño.

- La protección de datos personales en la Península Ibérica. Inmaculada Ramiro y Valentín Carrascosa.

- La LORTAD: análisis de su fundamento y de la jurisprudencia que la motiva. José Javier Santamaría Ibaes.

Ver también:

- "Los límites al derecho fundamental a la autodeterminación informativa en la Ley Española de Protección de Datos (LORTAD)", por Vicente López-Ibor Mayor. Actualidad Informática Aranzadi. nº 8. Julio 1993.

- "El derecho a la autodeterminación informativa", Erhard Deringer. Problemas Actuales de la Documentación y a Informática Jurídica. TECNOS 1987.

pio de reserva de ley establecido en el art. 53.1 de la Constitución; asimismo ha entendido que existe inconstitucionalidad en el art. 22.1 y en el primer párrafo del art. 22.2 por vulnerar el art. 18.4 en relación con el 18.1, al no respetar el contenido esencial del derecho al honor y a la intimidad personal y el 52.1 por igual motivo.

El Defensor del Pueblo, entendiendo que se producen los requisitos objetivos de inconstitucionalidad de la citada norma, y en uso de las atribuciones que la Constitución, la Ley Orgánica del Defensor del Pueblo y la Ley Orgánica del Tribunal Constitucional le confieren, interpuso el 28 de enero de 1993 recurso de inconstitucionalidad contra el artículo 19.1 y contra los incisos "funciones de control y verificación de las administraciones públicas" y persecución de "infracciones administrativas", así como contra el primer párrafo del artículo 22.2, todos ellos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, por estimar que vulneran el artículo 18.4 en relación con el art. 18.1 y el artículo 53.1 todos ellos de la Constitución española, recurso que se fundamentó en lo siguiente:

*PRIMERO. Inconstitucionalidad del artículo 19.1 de la Ley Orgánica 5/92 por no respetar el principio de reserva de ley establecido en el art. 53.1 de la Constitución.*

El art. 19.1 de la Ley Orgánica 5/92 de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, LORTAD, establece que:

*"Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán cedidos a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la cesión hubiese sido prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso".*

Por su parte el art. 18.1 de la misma norma dispone que:

*"La creación, modificación o supresión de los ficheros automatizados de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o diario oficial correspondiente".*

La cesión de datos personales sin consentimiento del titular de tales datos es una limitación al derecho a la intimidad. El art. 19.1 contiene una remisión en blanco, incondicionada y carente de límites ciertos y estrictos al ejecutivo para fijar los casos en los que proceda autorizarse la cesión de datos entre

administraciones públicas sin consentimiento del titular contraria al principio de reserva de ley proclamada en el art. 53.1 de la Constitución.

En el fundamento jurídico 3 de la sentencia 110/84 de ese alto tribunal se reflexiona en torno al contenido del derecho a la intimidad reconocido en el art. 18.1 de la Constitución en los siguientes términos:

*"... el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida".*

En el fundamento jurídico 3 del auto 642/86 se pone igualmente de manifiesto que:

*"El derecho a la intimidad que ha tenido acogida explícita en la Constitución con el carácter de fundamental, parte de la idea originaria del respeto a la vida privada personal y familiar, la cual debe quedar excluida del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado. En tal sentido, la Sentencia de este Tribunal 110/1984, tras aludir a las manifestaciones tradicionales de este derecho, en particular a la inviolabilidad del domicilio y de la correspondencia, se refiere a la extensión que ha experimentado la protección que de este derecho se deriva, como consecuencia de los avances de la técnica y del desarrollo de los medios de comunicación de masas, lo que obliga al reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida".*

En nuestro ordenamiento el "libre desarrollo de la personalidad" es "fundamento del orden político y de la paz social" al igual que la "dignidad de la persona" y los "derechos inviolables que le son inherentes", uno de los cuales es el derecho al honor y la intimidad personal y familiar, que como ha declarado este tribunal (STC 170/87, Fto. 4) "forman parte de los bienes de la personalidad que pertenecen al ámbito de la vida privada", y que por expreso mandato constitucional han de ser especialmente protegidos frente al uso de la informática.

En definitiva, el ciudadano debe poder controlar las cesiones de datos personales que se lleven a cabo entre diversos ficheros mediante el otorgamiento o no de su consentimiento al ser ello una garantía imprescindible ante

la potencialidad de la informática, pudiendo admitirse a este derecho tan sólo las excepciones proporcionadas y expresas que la ley prevea, puesto que las mismas suponen un límite al pleno ejercicio del derecho a la intimidad.

La lectura de la Ley Orgánica 5/92 revela que si bien a las normas que creen, modifiquen o supriman ficheros se les exige un determinado contenido -todo lo previsto en el art. 18.2- nada se concreta sobre cuáles sean los límites, las finalidades, las causas o las circunstancias en las que proceda establecer que sin consentimiento del afectado (art. 11.2.e) puedan cederse datos personales entre administraciones públicas. Tan sólo en el art. 7.3 se contiene una limitación específica que afecta a los datos de carácter personal que hagan referencia al origen racial, la vida sexual y la salud, los cuales sólo podrán ser cedidos "cuando por razones de interés general así lo disponga una Ley o el afectado consienta expresamente". Todos los demás datos personales que recojan las administraciones públicas, sean "sensibles" o no, afecten en mayor o menor medida a la intimidad de sus titulares o permitan conocer o no aspectos de su vida personal que el titular quiera mantener ocultos mediante su cruce con otros datos, pueden ser cedidos con el único requisito de que la norma de creación o modificación del fichero público -que será en muchos casos de rango reglamentario- así lo establezca.

Esta posibilidad, que surge de lo dispuesto en el art. 19.1 de la Ley Orgánica 5/92, convierte a este precepto en inconstitucional por no respetar el principio de reserva de ley establecido en el art. 53.1 de la Constitución.

*SEGUNDO. Inconstitucionalidad de los incisos "funciones de verificación y control de las administraciones públicas" y persecución de "infracciones administrativas" del art. 22.1 y primer párrafo del art. 22.2 de la Ley Orgánica 5/92 por vulnerar el art. 18.4 en relación con el 18.1 de la Constitución al no respetar el contenido esencial del derecho al honor y a la intimidad personal y familiar y el art. 53.1 de la norma fundamental por igual motivo.*

El art. 22 de la Ley Orgánica 5/92, de regulación del tratamiento automatizado de los datos de carácter personal, tiene una singular importancia puesto que regula las excepciones de los derechos de los afectados al acceso, rectificación y cancelación en relación con sus datos personales en el ámbito de los ficheros de titularidad pública.

Dicho precepto literalmente dice:

*"1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumpli-*



miento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la Seguridad pública o a la persecución de infracciones penales o administrativas.

2. Lo dispuesto en el art. 14 y en el apartado 1 del art. 15 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero automatizado invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas”.

A su vez, el art. 15.1 de la LORTAD dispone que:

“Los afectados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero automatizado 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 y cancelación.

e) De la identidad y dirección del responsable del fichero”.

Por su parte, el art. 14 de la misma Ley establece al regular el denominado derecho de acceso que:

“1. El afectado tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados.

2. La información podrá consistir en la mera consulta de los ficheros por medio de su visualización, o en la comunicación de los datos pertinentes mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos convencionales que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a los doce meses, salvo que el afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes”.

Finalmente, el art. 15 en su apartado 1 dispone en relación con los derechos de rectificación y cancelación que:

*“Por vía reglamentaria se establecerá el plazo en que el responsable del fichero tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del afectado”.*

El derecho a la información de los afectados se excepciona, entre otros casos, en aquellos en los que la información al afectado impida o dificulte gravemente el cumplimiento de “las funciones de control y verificación de las Administraciones Públicas” o a la “persecución de infracciones administrativas”. Asimismo, los derechos de acceso, rectificación y cancelación se excepcionan en el número 2 del art. 22 en aquellos casos en los que, ponderados los intereses en presencia, resultase que los derechos que dicho precepto reconoce a los afectados hubieran de ceder “ante razones pblico o ante intereses de terceros más dignos de protección”<sup>29</sup>.

En nuestra opinión, las restricciones establecidas en los párrafos entrecuadrados de este art. 22 suponen una vulneración del art. 18.4 en relación con

■ 29 Como señala José Antonio Martín Pallín (Magistrado del Tribunal Supremo), la Ley hace una diferencia entre los datos ultrasensibles y los meramente sensibles. Los primeros se refieren a la ideología religiosa y creencias y los segundos al origen racial, a la salud y a la vida sexual, permitiendo la recogida, el tratamiento, la automatización y cesión de estos últimos por razones de interés general o cuando lo disponga una Ley (art. 7) despojando al individuo de la custodia exclusiva y cesión voluntaria de estos datos.

Lo más significativo de la Ley radica en la diferencia de trato otorgada a los ficheros de titularidad pública en relación con los de titularidad privada. Los ficheros públicos gozan de una mayor permisividad en cuanto a la obtención, conservación y cesión de datos, mientras que los privados están sometidos a un régimen más estricto que garantiza suficientemente los derechos de los afectados.

Como ejemplo de esta diferencia podemos citar el art. 19.1 de la Ley que permite la cesión de los datos de carácter personal contenidos en los ficheros de las Administraciones Públicas, con la sola condición de que dicha cesión esté prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso. Este precepto puede resultar inconstitucional a tenor de lo dispuesto en el art. 18.4 en relación con el 53.1 y el art. 9.3 de la Constitución, que exige el respeto al principio de legalidad para las normas que afecten a los derechos fundamentales de la persona. El Defensor del Pueblo ha planteado recurso de inconstitucionalidad a instancia de la Comisión de Libertades e Informática. Uno de los aspectos más conflictivos de la Ley radica en el art. 20.2 y 3 que permite la recogida y el tratamiento automatizado, para fines policiales, de datos de carácter personal sin consentimiento de las personas afectadas sin ningún control judicial de la Agencia de Protección de Datos, en clara vulneración del art. 18.4 de la Constitución. Esta regulación ha suscitado un Recurso de Inconstitucionalidad presentado por el Partido Popular. La excepción se agrava con la limitación del derecho del ciudadano a la información sobre sus datos personales contenidos en los ficheros de las Administraciones Públicas (art. 31.1). Las excepciones a los derechos de los afectados se extienden a los supuestos que se relacionan con la Defensa Nacional, la Seguridad Pública o la persecución de infracciones penales o administrativas.

Tales excepciones las encontramos excesivas cuando se extienden a conceptos tan difusos como el “interés público” o “los intereses de terceros”. La negativa a facilitar, en estos casos, los derechos de acceso, rectificación y cancelación, incide en vicio de inconstitucionalidad y así lo ha estimado el Defensor del Pueblo al plantear Recurso sobre este punto ante el Tribunal Constitucional.



el 18.1 de la Constitución y del 53.1 de la misma norma fundamental al no respetar el "contenido esencial" del derecho fundamental, estableciendo excepciones que desnaturalizan el derecho al honor y a la intimidad personal y familiar de los ciudadanos en relación con el uso de la informática, e impidiendo que tal derecho sea reconocible como perteneciente al tipo descrito y sin que tales restricciones tengan justificación constitucional alguna.

Se solicita también la declaración de inconstitucionalidad del nº 2 del art. 22 de la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, en la medida en que en el mismo se prevén excepciones a los derechos de acceso, rectificación y cancelación -esto es, al "contenido esencial"- en aquellos casos en los que, ponderados los intereses en presencia, tales derechos de acceso, rectificación y cancelación hubieran de ceder "ante razones de interés público o ante intereses de terceros más dignos de protección".

Hasta aquí algunos de los argumentos más sobresalientes esgrimidos por el Defensor del Pueblo en este recurso. Pues bien, el error a nuestro juicio más importante de la Ley Orgánica 5/1992 es admitir un conjunto de excepciones y limitaciones al ejercicio de las facultades que conforman el derecho a la autodeterminación informativa, que dejan sin protección efectiva frente a los poderes públicos, el derecho fundamental regulado.

En este sentido, la norma aprobada se aparta de las excepciones previstas en el Convenio Europeo del Consejo de Europa, cuya importancia no sólo reside en el carácter internacional del Acuerdo, sino en el hecho de que por aplicación del art. 10 de nuestra Carta Magna, las normas relativas a los derechos fundamentales y libertades públicas se interpretarán de conformidad con los Tratados que sobre las mismas materias hayan sido ratificados por España (como se reconoce por diversas sentencias del Tribunal Constitucional, entre las que podemos destacar la 37/1988, de 3 de marzo, y 281/1991 de 14 de febrero).

La Ley contiene limitaciones discrecionales al derecho de autodeterminación informativa. La primera manifestación de dicho derecho se encuentra en el consentimiento del interesado respecto a la toma de sus datos personales, que opera en dos momentos temporales distintos: en la creación del fichero automatizado y en la cesión de datos a terceros<sup>30</sup>.

■ 30 Ver: Los límites al derecho fundamental a la autodeterminación informativa en la Ley Española de Protección de Datos (LORTAD), por Vicente López-Ibor Mayor. *Actualidad Informática Aranzadi*, nº 8, Julio 1993.

El art. 11.1 de la Ley, viene a establecer que la cesión de datos de carácter personal requiere el previo consentimiento del afectado, salvo (art. 19.1) que tratándose de datos recogidos o elaborados por las Administraciones públicas, no se cedan para el ejercicio de competencias diferentes; con la única excepción de que tal posibilidad estuviera prevista en la disposición de creación del fichero o por disposición posterior de igual o inferior rango que regule su uso. Cabría aquí de nuevo recordar que cualquier transferencia de datos de una instancia a otra no debería ser legítima sólo porque sea, a efectos administrativos, necesaria.

Una vez más se prevé la excepción de utilización discrecional, y se permite por vía reglamentaria la limitación del ejercicio de un derecho fundamental, en contra de lo sancionado en el art. 9.3 de la Constitución, y de la reserva de ley prevista en el art. 53.1.

El art. 22 establece los casos en que se excepciona el contenido mínimo garantizado para los mismos:

- Cuando se impida o dificulte gravemente el cumplimiento de las funciones de control o verificación de las Administraciones Públicas.

- Cuando afecte a la Defensa nacional.

- Cuando afecte a la Seguridad pública.

- Cuando afecte a la persecución de infracciones penales o administrativas.

Si bien las tres excepciones últimas están previstas en el art. 9 del Convenio de 1981; no lo está la primera de las citadas, que está regulada con un grado de generalidad de tal envergadura, -pues las funciones de control y verificación son inherentes a toda actuación administrativa, que entendemos no responde a la mínima exigencia constitucional requerida, vulnerando así el contenido esencial del derecho reconocido en el art. 18.4 de la norma fundamental española.