informática y DERECHO 6-7

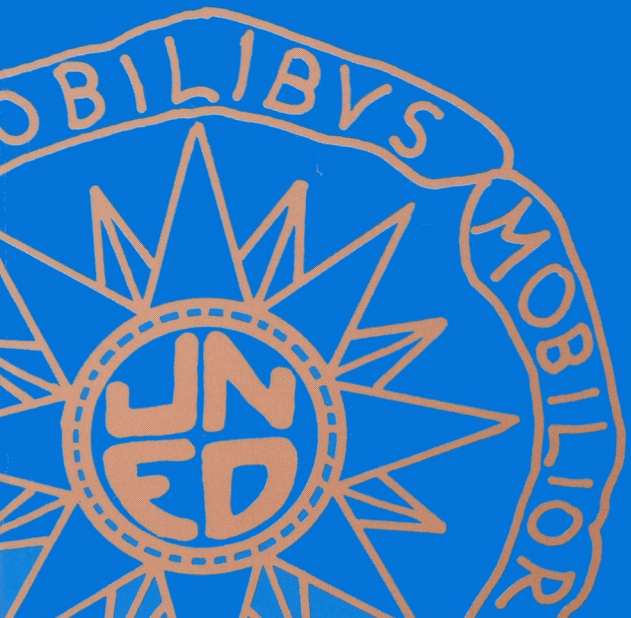
DIRECTOR: VALENTÍN CARRASCOSA LÓPEZ

LA PROTECCION DE DATOS PERSONALES

(EN LA L.O.R.T.A.D. Y DERECHO COMPARADO)

Movimiento Internacional de Datos
Autodeterminación Informática
Agencia de Protección de Datos
Seguridad y Confidencialidad
Los Derechos de las personas
- Información
- Consentimiento
- Acceso
- Rectificación
- Cancelación
- Indemnización

Infracciones y Sanciones
Ficheros Automatizados
Datos Sensibles



UNED
Centro Regional de Extremadura

informática Y DERECHO 6-7

DIRECTOR: VALENTÍN CARRASCOSA LÓPEZ

SOBRE LA EDICIÓN DIGITAL 2012

La presente edición es el resultado de un acuerdo de colaboración entre la *Federación Iberoamericana de Asociaciones de Derecho e Informática* (FIADI) y el *Instituto Chileno de Derecho y Tecnologías* (ICDT), formalizado en octubre de 2011 en la ciudad de Buenos Aires, en que se decidió re-editar digitalmente la que es la primera publicación periódica de habla castellana en Derecho Informático: **Informática y Derecho**, **Revista Iberoamericana de Derecho Informático**, que vio la luz en el año 1992 en el Centro Regional de Extremadura de la UNED de la ciudad de Mérida (España) bajo la dirección del Prof. Dr. Valentín Carrascosa López, y que dejó de publicarse tras una década de fructífera labor.

El objetivo final de esta nueva edición digital, ahora a cargo del *Instituto Chileno de Derecho y Tecnologías*, es rescatar los trabajos, investigaciones e ideas aparecidos en las páginas de esta revista académica para su libre consulta por futuras generaciones de docentes, investigadores y estudiantes, como modo de contribuir no solo con la preservación de la cultura jurídica, sino también aportar conocimiento a la historia de las ideas y rescatar la labor de los pioneros en temas de Derecho y Tecnologías en Iberoamérica.

informática Y DERECHO 6-7

DIRECTOR: VALENTÍN CARRASCOSA LÓPEZ

UNIVERSIDAD NACIONAL DE EDUCACION A DISTANCIA

Centro regional de Extremadura • Mérida

EDICION ORIGINAL IMPRESA

Universidad Nacional de Educación a Distancia
Centro Regional de Extremadura – Mérida
I.S.B.N.: 84- 88861 -51 – 6
Depósito Legal: BA- 299 - 1994
Impresión: Artes Gráficas Boysu, S. L. - Mérida

EDICIÓN DIGITAL 2012

Instituto Chileno de Derecho y Tecnologías
c/ Melchor Concha y Toro 187
7520312 Providencia,
Santiago de Chile
Web: http://www.icdt.cl

Sumario

PRESENTACION 9

VALENTIN CARRASCOSA LOPEZ
"La L.O.R.T.A.D.: Una necesidad en el panorama legislativo español" 11

ANTONIO ENRIQUE PÉREZ LUÑO
"La L.O.R.T.A.D. entre las luces y las sombras" 83

ALFONSO DE JULIOS CAMPUZANO
"Letra y Espíritu de la L.O.R.T.A.D.: ¿Un problema de coherencia interna?" 87

MIGUEL LÓPEZ-MUÑIZ GOÑI
"La Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal" 93

ALVARO SÁNCHEZ BRAVO
"La Regulación de los Datos Sensibles en la L.O.R.T.A.D." 117

MIGUEL ANGEL RAMOS
"La seguridad y la confidencialidad de la información y la L.O.R.T.A.D." 133

JORDI BACARIA
"El secreto estadístico: Contenido jurídico" 145

GUILLERMO OROZCO PARDO
"Los derechos de las personas en la L.O.R.T.A.D." 151

ANA ROSA GONZÁLEZ MURUA
"Comentario a la S.T.C. 254/1993, de 20 de julio, algunas consideraciones en torno al artículo 18.4 de la Constitución y la Protección de los Datos Personales" 203

EMILIO DEL PESO NAVARRO
"La figura del responsable del fichero de Datos de Carácter Personal en la L.O.R.T.A.D." 249

VICENTE LOPEZ-IBOR MAYOR
CARMEN PLAZA
"El Defensor del Pueblo: Derecho, Tecnologías de la Información y Libertades" 271

JOSEP JOVER I PADRO
"La abogacía y la L.O.R.T.A.D" 305

SANTIAGO RIPOLL CARULLA
"El Movimiento Internacional de Datos en la Ley Española de Protección de Datos" 313

MANUEL HEREDERO HIGUERAS
"La Agencia de Proteccion de Datos" 323

CINTA CASTILLO JIMÉNEZ
"Estatuto de la Agencia de Protección de Datos" 359

CARLOS M. ROMEO CASABONA
"Infracciones administrativas y penales en relación con la Protección de Datos" 365

STEWART H. DRESNER
Traductor: SANTIAGO RIPOLL CARULLA
"Panorama de la Legislación Europea sobre Protección de Datos Personales" 385

MARÍA LÁZPITA GURTUBAN
"Análisis Comparado de las Legislaciones sobre Protección de Datos de los Estados miembros de la Comunidad Europea" 397

AUDILIO GONZALES AGUILAR
Instrucciones de manejo del programa Informático IURILIEN. Bases de Datos Hypertexto aplicado a la L.O.R.T.A.D.....421

ANEXOS:

ANEXO I
"Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal. Hecho en Estrasburgo el 28 de enero de 1981"

ANEXO II.
"Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal"

ANEXO III.
"Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos"

ANEXO IV.
"Ley 78-17 del 6 de enero de 1978. Ley de Informática, Ficheros y Libertades". Francia

Presentación

Las Jornadas de Mérida, sobre la Ley del Tratamiento Automatizado de los Datos de Carácter Personal, "LORTAD", han supuesto la culminación y consolidación, de una vieja aspiración de muchos y, en especial, de la UNED extremeña, que con ello se apunta, con casi absoluta seguridad, a ser la primera institución española que organiza un encuentro, celebrado del 14 al 16 de julio de 1.993, sobre la LORTAD.

Con anterioridad ha habido jornadas que con esta línea se han organizado en Mérida. En cualquier caso, ahora con la ley en vigor, con una mayor y mejor profundización, este encuentro, ha servido de cauce para oir, conocer y discutir sobre una serie de cuestiones jurídicas, no exhaustivas, de las que desde hace tiempo y en especial hoy día preocupan no sólo a los estudiosos del Derecho sino también a los profesionales de este campo o de la informática y a todos los ciudadanos.

De los 2.071 profesionales que siguieron los 40 cursos impartidos en la VIII edición de la Universidad de Verano-93 de la UNED-Mérida, aproximadamente un centenar de ellos lo hicieron al XXII curso de Informática y Derecho: La Ley de Protección de Datos Personales, para analizar la LORTAD, y aquí está la publicación con sus reflexiones.

Aquí están las ponencias y comunicaciones que ponen de relieve todas las facetas más importantes de la LORTAD y que presentamos como obra colectiva.

Vaya, como punto final, mi gratitud a todos y cada uno de los colegas que han prestado su ayuda, su talento y su trabajo a este encuentro y cuyo fruto se recoje en este volúmen número 6 de "Informática y Derecho" que traemos a la luz con objeto de coronar y publicar el esfuerzo, la dedicación y el interés de tantas gentes para dar a conocer desde Extremadura, este problema tan candente y actual como es la protección de datos personales.

VALENTIN CARRASCOSA LOPEZ

LA LORTAD:
Una necesidad en el panorama Legislativo Español

VALENTIN CARRASCOSA LOPEZ
Doctor en Derecho
Licenciado en Ciencias de la Información

SUMARIO

I. INTRODUCCION

II. CONVENIO DE ESTRASBURGO

III. CONSIDERACIONES GENERALES

IV. RECURSOS DE INCONSTITUCIONALIDAD

A) DEL DEFENSOR DEL PUEBLO
B) DE LA GENERALIDAD Y PARLAMENTO DE CATALUÑA
C) DEL GRUPO PARLAMENTARIO POPULAR
D) CONCLUSIONES

V. EL RANGO NORMATIVO DE LA LORTAD

VI. NOTAS A LA L.O.R.T.A.D.

A) ESTRUCTURA DE LA LEY
B) EXPOSICION DE MOTIVOS
C) DISPOSICIONES GENERALES
   1. Objeto y Finalidad
   2. Ambito de la Aplicación
   3. Definiciones
D) PRINCIPIOS DE PROTECCION DE DATOS
   1. Calidad de los datos
   2. Recogida de datos
   3. El Consentimiento Afectado
   4. Datos especialmente protegidos
   5. Datos relativos a la Salud
   6. Cesión de los datos
E) DERECHO DE LAS PERSONAS
   1. Derecho de la Información
   2. Derecho de acceso
   3. Derecho de rectificación y cancelación
   4. Procedimiento
F) LOS FICHEROS
   1. Ficheros de Titularidad Pública
   2. Ficheros de Titularidad Privada
G) MOVIMIENTO INTERNACIONAL DE DATOS
H) AGENCIA DE PROTECCION DE DATOS
I) INFRACCIONES Y SANCIONES
J) DISPOSICIONES ADICIONALES, TRANSITORIA, DEROGATORIA Y FINALES

VII. LAS AUTOPISTAS DE LA INFORMACION

VIII. BIBLIOGRAFIA

I.- Introducción

Si a los XXV Cursos-Encuentros, sobre "INFORMATICA Y DERECHO", desarrollados en el Centro Regional de Extremadura de la UNED, unimos las jornadas, seminarios y Congreso que, sobre el tema, han tenido lugar en el mismo, nos haría suponer que la publicación de la LORTAD daría lugar a otro encuentro, por tratarse de un tema que nos venía preocupando desde hace muchos años, como quedó de manifiesto en 1.983, cuando, en Mérida, pronuncié conferencia sobre el tema que ya era y hoy en día es uno de los temas capitales de lo que se puede llamar, con matices importantes, Derecho de la Informática, Derecho Informático, Derecho de las Nuevas Tecnologías o Derecho de la Información, y en la que concluíamos insistiendo en la necesidad de esta Ley.

Con la publicación en el B.O.E. núm. 262, de 31 de Octubre de 1992, de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, "LORTAD", nos vemos impulsados a que pocos días después de su entrada en vigor, el 31 de enero de 1.993, se celebrase en Mérida, en julio de 1993, y dentro de su Universidad de Verano, un encuentro monográfico sobre el tema, en el XXII Curso dedicado íntegramente a la "LORTAD" y cuyas ponencias y comunicaciones van a constituir la base de esta publicación, pues se trata de un tema que traspasa las fronteras y forma parte del orden del día de la construcción europea, como lo demuestra la propuesta de directiva sobre esta materia presentada por el Consejo de las Comunidades el 13 de septiembre de 1990, o la propuesta de modificación de directiva 92/C 311/04 del Consejo, 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 (COM (92) 422 FINAL-SYN 287) y las numerosas reuniones, en Londres el 13 de Julio de 1993, Bruselas 28 y 29 de Octubre de 1993)... del grupo negociador de la propuesta de directiva marco de protección de datos (Syn 287).

Coincidimos con el profesor Pérez Luño[1], al afirmar que en el ambiente tecnológico de la sociedad contemporánea, todos los ciudadanos se hallan expuestos, desde su nacimiento, a ver perforada su privacidad por determinados usos de la informática y la telemática. La injerencia del ordenador electrónico en las distintas esferas y relaciones que configuran la vida cotidiana se ha hecho cada vez más extendida, difusa e implacable.

El control electrónico de los documentos de identificación, el proceso informatizado de datos sanitarios y fiscales, el registro de las adquisiciones comerciales realizadas con tarjetas de crédito, así como de las reservas de viajes, representan algunas muestras bien conocidas de la omnipresente vigilancia informática de nuestra existencia habitual. Ya que, en efecto, cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua o inadvertida que afecta incluso a los aspectos más sensibles de su vida privada; aquellos que en épocas anteriores quedaban fuera de todo control en su variedad y multiplicidad.

Estas proyecciones de la informática sobre la dignidad humana inciden contemporáneamente en los valores de la libertad y la igualdad. La libertad se ve mediatizada por técnicas informáticas de control individual y colectivo que comprometen gravemente su ejercicio en las sociedades más avanzadas. Al tiempo que, de forma simultánea, se produce un asalto a la igualdad, más implacable que en cualquier otra etapa histórica, al engendrarse una profunda disparidad entre quienes poseen o tienen acceso, al poder informático y quienes se hallan marginados de su disfrute.

Lo anterior no nos puede llevar a considerar, de una forma simplista y, por ende, falsa la que sólo viera en la informática una erosión o, en términos más radicales, una negación de los valores éticos jurídicos tradicionales, ya que las nuevas tecnologías más que abolir o desvirtuar los valores, han contribuido a redimensionar su significado y alcance, para situarlo a la altura de los parámetros de la sociedad postindustrial informatizada.

La aparición de esta sociedad postindustrial informatizada y los abusos cometidos, por falta de legislación específica, llevaron a los hechos denunciados por los medios de comunicación durante los últimos años y muy destacadamente durante los primeros meses de 1993, poniendo de manifiesto la existencia de una red de técnicos en informática que traficaban con datos personales de 21 millones de españoles, lo que representa la gravedad del nivel de

■ 1 PEREZ LUÑO, A.E. : "Impactos de la Informática en el sistema de valores Jurídicos", CITEMA 1987.

intrusión informática a la que podíamos estar sometidos los ciudadanos españoles.

Esta problemática no es exclusiva de los españoles, prácticamente todos los países avanzados se encontraban en idéntica situación de aquí que, en los últimos veinte años se haya intentado crear un cuerpo normativo, que partiendo de los años 70, momento en que el Estado de Hesse (República Federal Alemana) publica su célebre "Ley de Protección de Datos" (modificada en 1986) empezó a considerarse el riesgo que podía significar para el individuo la recopilación, ordenación y el uso de determinados datos relativos a la persona, hemos llegado a que las Cortes Generales hayan aprobado, recientemente, la Ley Orgánica 5/1992, de Regulación de Tratamiento Automatizado de los Datos de Carácter Personal "LORTAD".

La LORTAD llega tarde, pues tiene lugar al cumplirse el decimocuarto aniversario de aprobarse la Constitución española de 1978, en cuyo artículo 18.4 establece 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". El retraso de la ley podría verse compensado, si nos hallásemos ante una Ley moderna, que se beneficiase de la evolución de la doctrina e incorporase a ellas las normas dictadas a nivel internacional. Sin embargo el panorama que abre la LORTAD es bien distinto, ya que desde la discusión de la misma ha recibido contínuas críticas, por las numerosas excepciones, como la posibilidad de que los datos sensibles sean recogidos y tratados por las Fuerzas y Cuerpos de Seguridad del Estado sin ser necesario el consentimiento del afectado, o la dependencia gubernativa del Director de la Agencia de Protección de Datos. La tardanza no pone coto a las excepciones ni introduce normas en vigor en los países más avanzados en la materia, ello da lugar a que nada más entrar en vigor, haya sido objeto de cuatro recursos de inconstitucionalidad, presentados por el Defensor del Pueblo, la Generalidad de Cataluña, el Parlamento de Cataluña y el Grupo Parlamentario Popular.

Este retraso da lugar a la paradoja de que siendo España el segundo país europeo, después de Portugal, en reconocer constitucionalmente la necesidad de proteger a las personas frente a los riesgos de la informática ha sido uno de los últimos en establecer legislativamente los mecanismos que hacen posible tal protección, toda vez que en la década de los 70 aparecen Leyes de Protección de Datos Personales en Suecia (1973), Estados Unidos (1974), República Federal Alemana (1977), Canadá (1977), Francia, Dinamarca, Noruega y Austria (1978), Luxemburgo (1979) que consagran principios, definiciones, derechos y obligaciones en el campo del tratamiento automatizado de los datos personales y su repercusión sobre las actividades públicas, y en la misma línea

nos encontramos con mecanismos legislativos aprobados en la década de los 80 tales como la existencia de leyes que regulan la protección de datos personales en Canadá (Privacy act. 1982 que modifica la de 1977), Gran Bretaña (Ley 12 de Julio 1984), Islandia (Ley Nº 63, 1984), Israel (Ley 1981), Italia (Ley de 1 de Abril 1981), Suecia (Ley 1 de Julio 1982 que modifica la de 1973), Suiza (1981).

Si bien es cierto que la LORTAD llega tarde y mal también es cierto que concluye con una larga etapa de incertidumbres y vacios normativos, al tiempo que se inicia una serie de expectativas sobre las anheladas virtualidades de la misma para poner coto, y evitar en adelante, los abusos informáticos contra la intimidad perpetrados en nuestro país y que mientras el debate parlamentario de la LORTAD despertaron, dada su trascendencia, un ámplio interés, por lo que el texto aprobado merece un juicio moderadamente favorable y el texto en vigor puede conducir a un razonable nivel de protección de las personas frente al riesgo de la informática.

La LORTAD no nace sin embargo, por generación espontánea en España, la problemática social propiciada por la protección de la intimidad generó en fecha muy temprana la preocupación de la doctrina jurídica y de la Administración.

Como resultado de esta inquietud se produjeron, siguiendo al Profesor Ripol Carulla[2], diversas acciones del Gobierno y del legislador que hicieron de España pionera en la producción normativa sobre la temática. En concreto, España fue como hemos dicho, junto a Portugal, uno de los primeros países europeos en otorgar rango constitucional al "derecho de la protección de datos" (art. 18.4 de la Constitución).

Igualmente España fue uno de los cinco primeros países europeos en ratificar el Convenio del Consejo de Europa de 1981 y, asimismo, uno de los primeros Estados del continente en preparar, al comienzo de los 80, un proyecto de ley sobre el tema (el "Boletín Oficial de las Cortes Generales" en su número 1024-I de 24 de julio de 1980 publica un proyecto de Ley relativo al control de datos).

Sin embargo, los avances del legislador español se detuvieron en este punto. Al margen de otras consecuencias, esta pasividad determinó una situación de aparente indefensión del individuo ante una realidad cada vez más evidente, y que necesitaba el desarrollo del art. 18.4 de nuestra Constitución,

■ 2 RIPOL CARULLA, S.: "Introducción a la Protección de los Datos Personales", Centre d' Investigació de la Comunicació i Universidad Pompeu Fabra, 1993.

pues como ya decíamos en 1983[3], en el ordenamiento jurídico español no existían sino preceptos aislados, insuficientes tanto respecto a la protección del "Secreto informático" como del "derecho a la intimidad", por lo que concluíamos insistiendo en la necesidad de una pronta regulación de este tema ya que el problema que plantean los bancos de datos es acuciante y será muy grave, como ha ocurrido, en años venideros, pues en España no teníamos, salvo el mandato constitucional, ninguna Ley o jurisprudencia que reconociera a un particular el derecho de examinar, contestar, modificar o eliminar las informaciones que a él se refieran registradas en un banco de datos. No obstante saltaba a la vista que no era la mejor garantía que se le puede dar, pues como Niblett indica: en el medievo, cuando la prisión constituía la amenaza más grave que planeaba sobre las libertades individuales, apareció el principio del "Habeas Corpus" (procedimiento que no persigue la represión del delito, sino la solución o corrección de situaciones desacordes con la ley en materia de detención; su objetivo es la protección contra la detención ilegal). En nuestro tiempo, la libertad individual está amenazada de una nueva forma por el almacenamiento de bancos de datos de informaciones erróneas, incompletas, equívocas o caducadas, y por ello habría de adoptar un nuevo principio, el de "Habeas scriptum" ó "Habeas Data", autorizando al individuo a examinar los archivos que figuran bajo su nombre y a pedir las rectificaciones necesarias.

Esta situación, denunciada hace más de diez años, continuó hasta la promulgación, el pasado 31 de octubre, de la Ley Orgánica para la Regulación del Tratamiento Automatizado de los Datos de Carácter Personal "LORTAD", si bien, en nuestro ordenamiento hubo una serie de normas que sufrieron modificaciones, entre la aprobación de la Constitución y la LORTAD, tales como la Ley 62/1978, de 26 de diciembre, de protección jurisdiccional de los derechos fundamentales de la persona; la Ley 48/1978, de 7 de octubre, por la que se modifica la Ley de 5 de abril de 1968 sobre secretos oficiales; 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; la Orden de 30 de Julio de 1982 sobre limitación de acceso a la información contenida en las bases de datos fiscales; Ley Orgánica 3/1985, de 29 de mayo, sobre modificación de la Ley Orgánica 1/1982, de 5 de mayo sobre protección a la intimidad personal y familiar y a la propia imagen; Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de salud pública (arts. 2, 3 y 4); Ley 12/1989, de 9 de mayo, de la función estadística pública, etc.

■ 3 CARRASCOSA LOPEZ, V.: "Derecho a la Intimidad e Informática", Escuela Universitaria Politécnica, Mérida 1983.

Igualmente fueron ratificados, por España, convenios internacionales, que afectan al tema, tales como: el Instrumento de ratificación de 26 de septiembre de 1979, del Convenio de 4 de noviembre de 1950 para la protección de los derechos humanos y de las libertades fundamentales, enmendado por los Protocolos adicionales número 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966; Instrumento de ratificación de 27 de enero de 1984 del Convenio de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Hecho en Estrasburgo, y que constituye el primer texto internacional adoptado en este terreno. Es el fruto de cuatro años, en los cuales participaron expertos europeos, norteamericanos, australianos, canadienses y japoneses.

II.- Convenio de Estrasburgo

Aunque el Convenio de Estrasburgo se estableció bajo el patrocinio del Consejo de Europa, se encuentra firmado ya por más de treinta países y está abierto a la adhesión de países no europeos.

Su finalidad es, expresamente, la ordenación de la utilización de la Informática en la gestión de los datos personales de los ciudadanos.

Como decíamos[4], entre otras disposiciones, el texto estipulaba que "todo ciudadano debe beneficiarse de un derecho de inspección de las informaciones que le conciernen y que figuran en los ficheros informatizados". Si se comprueban errores, debe poder rectificar estas informaciones. Además, la Convención prohibe todo tratamiento de datos en que aparezca el origen racial, las opiniones políticas, las convicciones religiosas o la vida sexual. La Convención de Estrasburgo impone restricciones a la circulación internacional de datos, ya que técnicamente nada impide conservar en el extranjero ficheros relativos a la población de un país, para evitar que determinados organismos puedan transferir ficheros ilegales a países desprovistos de toda legislación que limite los usos de la informática. Así, a imagen de los paraísos fiscales, se podrían crear "paraísos informáticos", en donde todo estuviera permitido: todas las informaciones de ficheros, los tratamientos informáticos más peligrosos. A distancia, y gracias a la teleinformática, sería posible, por encima de las fronteras, interrogar fácilmente estos ficheros.

■ 4 CARRASCOSA LOPEZ, V.: "La correcta garantía del derecho a la intimidad". "La protección de los datos personales". Centre d'Investigació de la Comunicació i Universitat Pompeu Fabra. Barcelona, 1993.

El Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), redactado en Estrasburgo el 28 de enero de 1981 fue ratificado por España el 27 de Enero de 1984 y publicado en el B.O.E. el 15 de noviembre de 1985.

Si consideramos que el párrafo primero del artículo 96 de nuestra Constitución establece que "los tratados internacionales válidamente celebrados, una vez publicados oficialmente en España, formarán parte del ordenamiento interno..." y que la sentencia del Tribunal Constitucional de 20 de julio de 1993 reconoce eficacia directa e inmediata a los apartados a) y b) del artículo 8 del Convenio Europeo, al puntualizar que entre los derechos de los ciudadanos que se pueden ver afectados por el tratamiento de datos automatizados, existe uno, el derecho a conocer la existencia del fichero, su finalidad y la persona responsable del mismo, que constituye un prius para la defensa de los derechos reconocidos en el artículo 18.4 de la Constitución, podría hacernos reflexionar sobre la necesidad o no de la LORTAD.

El análisis de dicho precepto nos podría llevar a la conclusión de que la Convención de Estrasburgo, al formar parte del derecho interno, otorga derechos directamente ejercitables en España y que dicho Convenio releva al legislador de proceder al desarrollo del artículo 18.4 de la Constitución española, que preceptivamente dispone que: "La Ley limitará el uso de la informática para garantizar el honor a la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Conforme con el profesor Morales, este planteamiento es erróneo. En primer lugar, porque el artículo 4 de la Convención condiciona la efectividad de los principios fundamentales para la protección de datos personales al desarrollo por parte de cada uno de los estados de las medidas institucionales y jurídicas pertinentes.

Por otro lado, la Convención no puede constituir el desarrollo del artículo 18.4 de la Constitución, puesto que se trata de una normativa marco de principios que remite reiteradamente a las medidas legislativas de derecho interno. Además, el artículo 12 de la Convención condiciona la transmisión de datos personales informatizados al desarrollo de garantías de tutela del mismo, por lo que puede ser denegada esta transmisión de información por parte de cualquier Estado firmante del Convenio, si se comprueba la ausencia de medidas legislativas al respecto.

Hay que tener en cuenta, no obstante, el art. 10 de la Carta Magna, cuando establece que las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con los tratados y acuerdos sobre las mismas materias ratificadas por España y en

este sentido el propio Tribunal Constitucional se decanta por el valor interpretativo del Convenio, pues en el fundamento jurídico sexto de la sentencia 254/1.993 dice "... los textos internacionales ratificados por España pueden desplegar ciertos efectos en relación con los derechos fundamentales, en cuanto pueden servir para configurar el sentido y alcance de los derechos recogidos en la Constitución, como hemos mantenido, en virtud del art. 10.2 C.E., desde nuestra STC 38/81, fundamentos jurídicos 3º y 4º "....", pero no para sustituir el desarrollo del mismo por una norma interna".

El Convenio hecho en Estrasburgo, el 28 de enero de 1981, es de tal calado, que el Consejo de Europa, además de propiciar su redacción, ha dirigido desde el año 1985 varias recomendaciones a los Estados miembros en lo relativo a la protección de los datos personales, con un contenido material más concreto: datos utilizados por la Seguridad Social (1986), por la Policía (1987), comunicación a terceros de datos en poder de organismos públicos (1991), etc., y en la actualidad existe un documento de trabajo de los servicios de la Comisión de las Comunidades Europeas, cuyo objetivo es la recomendación de decisión del Consejo sobre la apertura de negociaciones con vistas a la adhesión de las Comunidades Europeas al Convenio del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de datos personales (Convenio 108).

Aunque la mayoría de los Estados miembros (10 de 12) son partes contratantes del Convenio 108, entre ellas como hemos visto España, existen fundados motivos para considerar que una adhesión de la Comunidad reforzaría el interés de los terceros países por este Convenio. La elaboración del proyecto de Directiva suscita en varios paises un interés manifiesto, especialmente en lo que se refiere a las disposiciones sobre los flujos transfronterizos. Cabe pensar que estos paises, en un marco intergubernamental, desearan equiparar su experiencia en materia de protección de datos personales con la política comunitaria que defina la Directiva. El principio de libre circulación que establece el Convenio, aunque esté sujeto a las excepciones del apartado 3 del artículo 12, puede resultar más atractivo que la aplicación unilateral, por la Comunidad, de su propia normativa. El convenio 108 podría constituir la base de un foro internacional, que podría ampliarse a socios no europeos de la Comunidad, tal como lo permite el artículo 23 del Convenio.

Entre los motivos para la adhesión de la Comunidad al Convenio 108, podemos citar el de que en su calidad de persona jurídica de derecho público, con capacidad para contraer compromisos internacionales, la Comunidad debe asumir de cara al exterior las consecuencias de su evolución interna y dar el respaldo al único texto internacional vinculante en vigor, reforzando el inte-

rés del Convenio 108 para los terceros paises que deseen mantener con la Comunidad relaciones comerciales con la mayor libertad posible.

La adhesión al Convenio 108 garantizará en principio la libre circulación de datos entre la Comunidad y terceros paises que suscriban el Convenio, con la correspondiente protección de las personas, se creará de este modo un ámplio espacio geográfico de libre circulación, imprescindible para el desarrollo del comercio internacional.

Si la Comunidad, por el contrario, no se adhiere al Convenio, puede existir, tras la aprobación de la Directiva, un riesgo de parálisis de las instancias del Convenio 108, al menos para los ámbitos que son competencia de la Comunidad, pues ésta no podría ejercer sus competencias y los Estados miembros, aunque sean parte del Convenio, no podrían suscribir compromisos sobre lo dispuesto en la Directiva, por lo que en la medida en que los terceros paises no se opongan a la adhesión de la Comunidad, ésta deberá adherirse al Convenio para ejercer sus competencias, de conformidad con el Tratado, con la jurisprudencia reiterada del Tribunal de Justicia y con la práctica de las competencias exteriores, lo lamentable es que el procedimiento se halla en la primera etapa o de recomendación de la Comisión al Consejo para que le autorice a iniciar negociaciones, en nombre de la Comunidad.

En la reunión de 14 de septiembre de 1993, casi todas las delegaciones se preguntaron si era oportuno que el Consejo iniciara una labor en este ámbito, cuando todos los esfuerzos deberían concentrarse en la aprobación de una posición común sobre la propuesta de Directiva. Les pareció preferible, tanto para la definición de las prioridades del Consejo como para la posición del negociador, que se esperase a la adopción de la posición común, que se producirá, previsiblemente, en el transcurso de 1994.

Independientemente de las directrices negociadoras, el momento, y la forma de adhesión si vamos a recoger los efectos de la adhesión, ya que, cuando ésta se produzca, en virtud del apartado 7 del artículo 228 del Tratado CEE, los acuerdos celebrados por la Comunidad son "vinculantes para las instituciones de la Comunidad así como para los Estados miembros". De acuerdo con la jurisprudencia del Tribunal de Justicia, son parte integrante del ordenamiento jurídico comunitario y por tanto el acuerdo celebrado por la Comunidad gozará de la primacía que se le reconoce al derecho comunitario. Por consiguiente, los tribunales nacionales deben aplicarle frente a las leyes nacionales que le sean contrarias. Al ser un elemento del derecho comunitario, puede ser objeto de un recurso prejudicial ante el Tribunal de Justicia y llegado el caso, el convenio 108 podría invocarse ante el Tribunal de Justicia, en un litigio entre

una institución y un particular, cuyos datos personales hubiesen sido tratados en infracción de las normas contenidas en el mismo.

Teniendo en cuenta que el Convenio ya ha sido suscrito por la mayoría de los paises de la Comunidad, la adhesión de la Comunidad al Convenio 108 lo convertiría en un "acuerdo mixto" suscrito tanto por la Comunidad como por los Estados miembros, pero habrá que esperar al final del procedimiento y a su aprobación o no y en consecuencia, caso de celebrarlo, a su publicación en el Diario Oficial de las Comunidades Europeas.

El Convenio, supone la regulación mínima que debe ser desarrollada por las normas internas que cada Estado dicte después de la notificación y así la LORTAD lo que pretenda es cumplir tanto con el mandato constitucional contenido en el art. 18.4 de la Constitución Española como con el art. 4 del Convenio de Estrasburgo y atender como dice en la exposición de motivos, a las exigencias y previsiones que se contienen en el Consejo de Europa para la protección de las personas con respecto al tratamiento de los datos de carácter personal.

III.- Consideraciones Generales

Todo ello nos lleva no sólo a la conveniencia sino mejor a la necesidad de la publicación de la LORTAD (que había sido precedida, desde 1980 en que se formula en el Congreso una pregunta, por el Diputado Sr. Fraga Iribarne, sobre la necesidad de un proyecto de ley de datos, por preguntas, comparecencias, proposiciones no de ley y proposiciones de ley), por mandato expreso del artículo 18.4 de la Constitución, y el Convenio internacional ratificado por España, pero, como hemos apuntado anteriormente, tarde y con algunas deficiencias que pudieron y debieron ser evitadas al contar con las experiencias previas del Derecho comparado.

La LORTAD, colma, no obstante, una importantísima laguna legal de nuestro ordenamiento jurídico ampliamente sentido por la opinión pública, y que esta ley regulariza al permitir, a los afectados, del derecho de información y acceso a los datos y del derecho de rectificación y cancelación, así como de los principios relativos a la calidad de los datos, a la información sobre su recogida, al consentimiento, a la seguridad y a la cesión de los mismos, en una palabra, a establecer un arsenal de garantías y derechos dentro de un marco normativo, como es la LORTAD que pone fin a las respuestas fragmentarias y marginales para la tutela de la libertad informática de las personas que nuestro ordenamiento jurídico contenía.

Esta Ley contiene modificaciones y logros importantes, como los ya anunciados de acceso de los interesados a los datos y las garantías sobre la rectificación y uso de los mismos, a los que podríamos añadir otros más tales como: la calidad y transparencia, que unido al consentimiento y la tutela reforzada de los datos sensibles son aciertos, pero igualmente hay muchos puntos negros, tales como: posible vulneración del espíritu y letra de la Constitución (no podemos olvidar que hay varios recursos de inconstitucionalidad, planteados por el Defensor del Pueblo, Generalidad de Cataluña, etc.), excepciones injustificadas y no controladas de aplicabilidad, desajuste respecto a la legislación comparada, etc. La mayoría de estos temas serán expuestos en los trabajos aquí recogidos pero nosostros querríamos hacer unos pequeños comentarios sobre lo que consideramos más digno de destacar, y la primera duda que se nos plantea es la de considerar si esta Ley nace en virtud del mandato constitucional y convenio de Estrasburgo, para proteger efectivamente a las personas o por el contrario se trata de cumplir, sin pérdida de tiempo, cuando lo impone un Convenio como el de Schengen, cuyo objetivo no es precisamente la protección de los derechos humanos, sino la autoprotección de los Estados y la cooperación en materia de control de fronteras y persecución de delincuentes, por conveniente que pueda considerarse el acuerdo de adhesión del Reino de España al convenio de aplicación del acuerdo de Schengen de 14 de Junio de 1985, entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal Alemana y de la República Francesa, relativo a la supresión gradual de controles en las fronteras comunes, firmado en Schengen el 19 de Junio de 1990 (BOCG, Senado, Serie IV, de 20 de febrero de 1992).

Nos preguntamos en estas consideraciones generales ¿Estamos ante una verdadera Ley de protección de datos o con ella sólamente se busca cubrir formalmente una obligación, pero con un escaso compromiso de fondo? Los comentarios posteriores nos ayudarán a inclinarnos por una u otra postura pero reiteramos una vez más que con ella concluye una larga etapa de incertidumbre, y de vacíos normativos por lo que el texto puede conducir a una razonable protección de las personas frente al abuso informático, aunque este no hubiese sido el objetivo del legislador.

IV.- Recursos de Inconstitucionalidad

Entre los puntos negros, hemos señalado, en primer lugar, la posible vulneración del espíritu y letra de la Constitución, suficientemente moderna como para conocer la importancia del establecimiento de límites efectivos que impongan barreras al manejo de los datos informáticos que afecten al pleno ejercicio de los derechos fundamentales de la persona, de aquí que recojamos,

someramente, algunos de los argumentos esgrimidos en los recursos de inconstitucionalidad planteados.

A) DEL DEFENSOR DEL PUEBLO

El 28 de Enero de 1993 el Defensor del Pueblo, planteó ante el Tribunal Constitucional el correspondiente recurso de inconstitucionalidad, que también le habían solicitado varias instituciones: Comisión de Libertades e Informática, Confederación Sindical de Comisiones Obreras, Unión General de Trabajadores y portavoz del grupo parlamentario de Izquierda Unida de la Asamblea Regional de Murcia.

Tras los informes jurídicos elaborados por los servicios compententes de la institución, la Junta de Coordinación y Régimen Interior, en reunión de 26 de enero de 1993, y según determina el art. 18.1 b del Reglamento de Organización y Funcionamiento del 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, interpone demanda de recurso de inconstitucionalidad contra el **apartado 1, del artículo 19**, y los incisos "funciones de control y verificación de las administraciones públicas" y persecución de "infracciones administrativas", **del artículo 22.1**, y asimismo contra el primer párrafo del **artículo 22.2** todos ellos de la Ley Orgánica 5/92, de 29 de Octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, por considerar que a través de los mismos se vulneran los artículos 18.4, en relación con el 18.1 y el 53.1 de la Constitución española.

Como hemos recogido, en el párrafo anterior, los motivos de inconstitucionalidad alegados se fundan en la inconstitucionalidad del artículo 19.1, por no respetar el principio de reserva de Ley establecida en el artículo 53.1 de la Constitución.

El Defensor del Pueblo hace en su escrito un estudio de diversos preceptos de la LORTAD, tales como la exposición de motivos, que afirma que "para la adecuada configuración, que esta Ley se propone, de la nueva garantía de la intimidad y del honor, resulta esencial la correcta regulación de la cesión de los datos almacenados", ya que según advierte esta exposición de motivos es el cruce de datos lo que puede agredir los límites de la privacidad, motivo por el cual "la Ley completa el principio del consentimiento exigiendo que, al procederse a la recogida de los datos, el afectado sea debidamente informado del uso que se les puede dar, al objeto de que el consentimiento se preste con conocimiento cabal de su exacto alcance, pero la Ley se aleja de estas loables

intenciones, al menos en lo que se refiere a los datos personales recogidos o elaborados por las administraciones públicas, cuyo régimen de cesión dista de ser el propio del denominado "principio del consentimiento" completado por el de "información" al afectado, ya que si bien se establece el principio general de que los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos con el consentimiento previo del afectado (art. 11.1.) tal principio se excepciona inmediatamente para las administraciones públicas con el único requisito de que lo prevea la norma general que cree el fichero u otra posterior de igual o superior rango que la modifique (art. 19.1).

En efecto, la disposición general que crea o modifica un fichero de titularidad pública no está sometida a limitación específica alguna a la hora de establecer cesiones de datos de carácter personal a otras administraciones públicas. Es necesario tan sólo que la autoridad competente para dictar la norma reglamentaria, considere oportuno que se lleve a cabo la cesión de datos personales para que, amparada por el texto del art. 19.1 de la LORTAD en relación con el 18.1, pueda aprobar la norma correspondiente y establecer esta limitación al derecho de las personas.

Se apoya el recurso no sólo en los artículos citados sino también en el art. 18.1.4 y 19.1, así como en los artículos 10.2, 5 y 8 del Convenio de Estrasburgo y fundamentalmente en el principio de reserva de ley contenido en el artículo 53.1 de la Constitución y en numerosas sentencias del Tribunal Constitucional español, tales como 6/81, 11/81; 83/84, 110/84 y 196/87, que sientan el principio de que la cesión de datos de carácter personal sin el consentimiento de su titular supone el establecimiento de un límite a su derecho fundamental a la intimidad y que el art. 19.1 de la LORTAD autoriza a que dicho límite sea impuesto por normas de rango reglamentario, vulnerando el art. 53.1 de la Constitución, ya que el artículo 19.1 contiene una remisión en blanco, incondicionada y carente de límites ciertos y estrictos al ejecutivo para fijar los casos en los que se proceda autorizarse la cesión de datos entre administraciones públicas sin consentimiento del titular contraria al principio, como hemos apuntado, de reserva de Ley proclamada en el artículo 53.1 de la Constitución.

La sentencia 110/84 del Tribunal Constitucional reconoce un derecho global a la intimidad y vida privada y un respeto a la vida privada y familiar, que debe quedar excluida del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado, pero igualmente ha declarado dicha sentencia que "no existen derechos ilimitados", ya que "todo derecho tiene sus límites que en relación a los derechos fundamentales establece la Constitución por sí misma en algunas ocasiones, mientras en otra el límite se deriva de una manera mediata e indirecta de tal norma, en cuanto ha de justificarse por la

necesidad de proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionalmente protegidos".

El individuo tiene, pues, que aceptar en principio determinadas limitaciones de su derecho a la autodeterminación informativa en aras del interés preponderante de la colectividad, conforme determina el Tribunal Constitucional Federal Alemán, en Sentencia de 15 de diciembre de 1983, argumentada reiteradamente en el recurso y de la que también transcribe que "un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia, y en esta medida ya no existe, bajo las condiciones de elaboración automática de datos, ningún dato "sin interés", ya que todos éstos forman parte del derecho fundamental a la intimidad cuando se ejercita éste ante el tratamiento automatizado de datos personales por parte de las administraciones públicas, la capacidad del titular de tales datos de consentir o no la cesión de los mismos, suponiendo la limitación de esta capacidad un límite al ejercicio del derecho que por imperativo del artículo 53.1 de la Constitución ha de venir regulado por Ley.

En conclusión, 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 artículo 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 artículo 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 establezcan.

Esta posibilidad es lo que ha llevado al Defensor del Pueblo a recogerlo como motivos de inconstitucionalidad por no respetar el principio de reserva de Ley establecido en el art. 53.1 de la Constitución.

B) DE LA GENERALIDAD Y PARLAMENTO DE CATALUÑA

Los recursos de inconstitucionalidad no sólamente se centran en los arts. 19 y 22, a que se refiere el formulado por el Defensor del Pueblo, relativos a la

cesión de datos y a otras excepciones a los derechos de los afectados, es decir, a conceptos muy importantes y generales, sino que también la Generalidad de Cataluña y el Parlamento de Cataluña formulan recursos de inconstitucionalidad respecto a otros artículos tales como el **24**, **31**, **40.1** y **40.2** que se incluyen en los recursos de ambas instituciones más el recurso contra el art. **39** que sólamente lo recoge la Generalidad de Cataluña.

En los recursos de las instituciones catalanas se indica que la Ley desconoce, y por ello niega, las competencias de las Comunidades Autónomas en relación a los ficheros de titularidad privada y otorga, con carácter exclusivo, las facultades de inscripcion de los códigos tipo a que se refiere el artículo 31 al Registro General de protección de Datos, excluyendo, en consonancia con los artículos 24 y 40.2 de la Ley, que las Comunidades Autónomas ejerzan en toda su extensión las competencias que les atribuye el bloque de la constitucionalidad.

Igualmente alegan que de la lectura del apartado 1 del artículo 40 se desprende que las Comunidades Autónomas son competentes para crear órganos a los que se garantizará plena independencia y objetividad en el ejercicio de su cometido, toda vez que dicho precepto establece:

"1.- Las funciones de la Agencia de Protección de Datos regulada en el artículo 36, 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 45 y 48, en relación con sus específicas competencias, serán ejercidas, cuando afecten a ficheros automatizados de datos de carácter personal creados o gestionados por las Comunidades Autónomas, por los órganos correspondientes de cada Comunidad, a los que se garantizará plena independencia y objetividad en el ejercicio de su cometido.

2.- Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros públicos para el ejercicio de las competencias que se les reconoce sobre los mismos, respecto de los archivos informatizados de datos personales cuyos titulares sean los órganos de las respectivas Comunidades Autónomas o de sus Territorios Históricos".

De la lectura detenida del mismo alegan que el problema no estriba en la lista de funciones que pueden asumir las Comunidades Autónomas y las que se reserva el Estado a través de la Agencia de Protección de Datos, sino en que el artículo 40.1 formula la atribución en un doble sentido: en primer lugar establece que las funciones serán ejercidas por las Comunidades Autónomas "en relación con sus específicas competencias", pero esta afirmación, correcta y

respetuosa con el reparto competencial establecido en el bloque de la constitucionalidad, queda desnaturalizada por un segundo inciso que determina que las funciones atribuidas a las Comunidades Autónomas sólo pueden ser ejercidas "cuando afecten a ficheros automatizados de datos de carácter personal creados o gestionados" por éstas, es decir, limitando la competencia de la Comunidad Autónoma en función de la titularidad del instrumento, excluyendo por tanto aquellos archivos de titularidad privada cuya finalidad y cuyo uso se enmarcan en una competencia sustantiva de la Comunidad Autónoma.

El objeto de estos recursos de inconstitucionalidad se concretan, por tanto, en la reivindicación de la competencia de las Comunidades Autónomas para el ejercicio de las referidas potestades y funciones de tutela sobre los ficheros de titularidad privada o de la Administración Local de Cataluña.

En sus fundamentos jurídicos parten del precedente alemán y en la creación del "Datenschutzbeauftragter" en 1970 al aprobarse la Ley de Protección de Datos de el Land de Hesse (R.F.A.), para continuar con el estudio de sentencias del Tribunal Constitucional Español, y en especial de la LORTAD, que contiene una parte, con rango de Ley Orgánica, cuyo objetivo es el desarrollo de los derechos fundamentales, y una segunda parte, con rango de Ley ordinaria, donde, esencialmente se regula el control administrativo de aquellas actividades, para continuar hablando de la competencia residual que, por aplicación del art. 149.3 de la Constitución Española, corresponda automáticamente al Estado, para poner igualmente de manifiesto la naturaleza administrativa de la Agencia de Protección de Datos, que excluye toda posibilidad de que la reserva íntegra de la Agencia de Protección de Datos de la tutela sobre ficheros de titularidad privada o local pueda legitimarse competencialmente en el art. 149.1 de la C.E.

La inconstitucionalidad la plantean fundamentalmente porque el art. 40 de la LORTAD reconoce expresamente tan sólo las competencias de las Comunidades Autónomas respecto de la protección de datos relativos a ficheros creados o gestionados por ellas mismas y, por tanto de titularidad pública, quedando excluido el reconocimiento de las competencias autonómicas sobre los ficheros de titularidad privada y local, impidiendo por tanto los artículos impugnados la creación y mantenimiento por las Comunidades Autónomas de Registros de Protección de Datos en los que se inscriban los ficheros automatizados que puedan crear personas o entidades privadas en su territorio, ya que conforme a la Disposición final tercera de la LO 5/1992, el artículo 24 goza del carácter de Ley Orgánica y éste establece la necesidad de previa notificación a la Agencia de Protección de Datos y su inscripción, por ésta, en el Registro General de Protección de Datos, de la creación de ficheros automatizados

de datos de carácter personal, o su modificación por parte de personas o entes privados.

De la función inspectora han quedado excluidas las Comunidades Autónomas, que el artículo 39 atribuye a la Agencia de Protección de Datos.

C) DEL GRUPO PARLAMENTARIO POPULAR

Al igual que el Defensor del Pueblo e Instituciones Catalanas el Grupo Parlamentario Popular interpuso recurso de inconstitucionalidad contra los artículos **6.2, 19.1, 20.3, 22.1, 22.2,** y los demás que procedan por conexión, de la Ley Orgánica 5/1992,de 29 de octubre de Regulación del Tratamiento Automatizado de Datos de Cáracter Personal.

Estructuran su recurso en dos partes, lo que supone sin duda una modificación formal respecto a los escritos de esta naturaleza. La primera parte del recurso tiene por objeto hacer una breve síntesis de lo que ha significado en algunos países del mundo occidental, y en particular en Alemania, y lo que significa en nuestro sistema jurídico el establecimiento, por la Constitución, de la necesaria existencia de límites al poder informático, en defensa de los derechos al honor, intimidad personal y familiar de los ciudadanos, y el pleno ejercicio de sus derechos, y por tanto la consagración de un nuevo derecho fundamental: el derecho a la autodeterminacion informativa.

Derecho fundamental que se encuentra en fase de formación, elaboración y, lo que es más sustantivo, afirmación constitucional, para la que la resolución de este recurso tendrá importancia decisiva.

Matiza, su recurso, haciendo constar que hace menos de veinte años este derecho fundamental no sólo no existía, sino que no era necesario, ni siquiera posible su existencia. El desarrollo tecnológico de las sociedades y sus implicaciones sociales y jurídicas encuentran ahora en el mundo contemporáneo evidentes niveles de penetración y múltiples consecuencias. Entre ellas, como una de las más relevantes, es el efecto sobre los datos personales y su procesamiento electrónico en manos de terceros, cualquiera que sea la naturaleza jurídica de estos sujetos, pública o privada.

El derecho tiene ante todo un carácter dinámico derivado de la propia realidad tambien cambiante sobre la que históricamente se proyecta y de aquí que la primera parte de este recurso sea descriptiva y conceptual y, por tanto, poco convencional, por el carácter novedoso de la cuestión planteada.

La segunda parte tiene por objeto desarrollar los motivos de inconstitucionalidad, y por tanto se ajusta a la construcción formal de este tipo de recursos.

Atendiendo al planteamiento del recurso en su primera parte analiza:

- la naturaleza del derecho de protección de la intimidad personal.

- Alcance del derecho de protección de la intimidad personal. Puntualizando que el derecho fundamental de proteccion de la intimidad trata de proteger la esfera personal del individuo en relación con su propia vida (tanto a aspectos corporales como a aspectos incorporales-sentencia del Tribunal Constitucional de 27 de junio de l.990) y en relación con la vida del hombre respecto a los otros(mantenido por el Tribunal Constitucional en la Sentencia de l7 de octubre de l.991).

- Protección jurídica del derecho a la Intimidad. (Se hace mencion al primer texto legislativo español, posterior a la Constitución que protege de manera unitaria los derechos de la vida privada, es decir la Ley 62/l.978, de 26 de diciembre, de protección jurisdiccional de los Derechos fundamentales de la persona; 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,asi como a la sentencia de l2 de noviembre de l990 del Tribunal Constitucional, para hacer igualmente un recorrido por el Código Penal y en especial por los artículos l92, 497, 498, 360, 367 y 368 que tipifican conductas que se refieren al secreto de las comunicaciones, a la inviolabilidad del domicilio (art. l9l, 49 y ss) los artículos 253 y 457 que regulan la calumnia y la injuria, para concluir con la necesidad de una protección procesal adecuada, de modo que cualquier ciudano pueda recabar la tutela de los derechos fundamentales y libertades públicas, no sólo por el procedimiento ordinario, sino por los procedimientos sumarios previstos en el artículo 53 de la Constitución y por el recurso de amparo ante el Tribunal Constitucional.

- La doble vertiente del derecho a la intimidad. El derecho a la intimidad, tradicionalmente definido como un derecho esencialmente negativo, presenta rasgos nuevos y distintos en las sociedades tecnológicamente avanzadas, no abarcando ya su estudio únicamente el de un derecho configurado de un ámbito de no invasión o no interferencia, sino que se viene a perfilar con un contenido abiertamente positivo. No es, pues un derecho garantista frente a las invasiones indebidas o ilícitas en la esfera privada, sino que cabe contemplarlo también como un derecho activo de control sobre el flujo de informaciones referentes a uno mismo. La intimidad se manifiesta así como un derecho o

facultad de autodeterminación informativa, y la informática conoce un doble límite: el de la necesaria interdicción de los datos -principalmente de aquéllos calificados como "sensibles"-, y el que viene dado por el derecho de las personas a acceder a los datos poseidos sobre ellos y controlar su posible divulgación.

Actualmente, como ha señalado Vittorio Frosini, el derecho a la intimidad es el derecho a proteger los datos que pertenecen al individuo.

- Leyes sobre Protección de Datos en el Derecho comparado. Hacen una breve referencia a algunas disposiciones sobre protección de datos en el Derecho comparado, partiendo de la Ley orgánica 78/17, de 1978 francesa, en la que se consagran principios, definiciones, derechos y obligaciones en el campo del tratamiento automatizado de los datos personales y su repercusion sobre las actividades públicas, para pasar a los Estados Unidos donde destaca la "Privacy Act" de 1974 y la "Data Protection Act" de 1984 y a la Ley Alemana de 1977, Austríaca de 1978, Canadá de 1982, Dinamarca (1978), Gran Bretaña (1984), Islandia (1984), Israel (1981), Italia (1981), Luxemburgo (1979), Suecia (1.982), Suiza (1.981).

- El Convenio del Consejo de Europa para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, merece una especial atención y así lo hacen al igual que dos resoluciones sobre protección de la vida privada de los individuos, con respecto a los bancos de datos electrónicos que el Comité de Ministros del Consejo de Europa adoptó en 1973 y 1974.

- La sentencia del Tribunal Constitucional alemán de 15-12-1983, sobre la Ley del Censo: el derecho fundamental a la autodeterminación informativa o libertad informática tiene capítulo inportante por marcar el punto más preciso en la construcción del derecho a la autodeterminación.

Son numerosas las consideraciones de interés que recoge la citada Sentencia del Tribunal Constitucional alemán, entendemos preciso, sin embargo, resumirlas en dos de sus trazos o vertientes más relevantes: Un primer término en su relación o vinculación con la libertad y dignidad humanas y, en segundo lugar, en su relación con los valores democráticos.

Como hemos apuntado anteriormente la segunda parte del recurso tenía por objeto desarrollar los motivos de inconstitucionalidad, por violación del artículo 18.4 de la Constitución, en relación con los arts. 105.b y 10 del mismo cuerpo legal, en cuanto que, en el contexto de los derechos al honor, la intimi-

dad personal y la propia imagen -y por tanto, en el contexto de la libertad informática y el derecho a la autodeterminación informativa-, establece que la ley limitará el uso de la informática para garantizar los mencionados derechos, y en realidad la nueva Ley 5/1992 vacía sus supuestas limitaciones de contenido efectivo, haciéndolos inoperantes frente a las Administraciones Públicas.

Nuestra Constitución es suficientemente moderna como para conocer la importancia del establecimiento de límites efectivos que impongan barreras al manejo de los datos informáticos que afecten a estos derechos y así lo hace, pero nuestro texto constitucional adolece de cierta imprecisión al no definir con claridad los contornos de este nuevo derecho de la personalidad, pero no cabe duda que la expresión "limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos" no puede tener otro significado que el deseo del poder constituyente de otorgar a los ciudadanos unas posibilidades de actuar en un doble sentido:

- **poder pedir o prohibir** cualquier intromisión ilegítima en la esfera privada de su intimidad a través del uso de las nuevas tecnologías informáticas.

- **garantizar el ejercicio** de las facultades de conocer y acceder a las informaciones incorporadas a una Base de Datos personales (habeas data o habeas scriptum), corregir o suprimir los datos inexactos o inválidamente procesados y disponer sobre su transmisión.

Se transcriben palabras de Martín Toval cuando se aprobó el art. l8 de la Constitució n; ilustrativamente ponen el ejemplo del programa "Safari"frances que despues de una campaña de opinión muy extensa y polémica y de un amplio debate parlamentario, no pudo ser aplicado por el Ministerio del Interior.

Para los recurrentes la Ley Orgánica impugnada es inconstitucional por cuanto, en los artículos que impugnan como inconstitucionales, establece un conjunto de excepciones, establecidas en forma de conceptos jurídicos indeterminados, que dejan la protección efectiva del derecho fundamental -el límite, que la Constitución impone, precisamente para proteger el Derecho- en manos de la Administración Pública, de tal modo que se vacían plenamente de contenido, en relación con los ficheros automatizados de la Administración Pública, el contenido de los derechos al honor, intimidad personal y familiar de los ciudadanos, y el pleno ejercicio de sus derechos fundamentales. Porque los límites, cuyo establecimiento la propia Constitución impone, son -en la práctica- inexistentes. No hay límites, sino otorgamiento de unas absolutas facultades de discrecionalidad. Discrecionalidad que vacía de contenido la

Constitución por cuanto remite infaustamente al contenido efectivo de los límites reales al poder informático no ya a una norma reglamentaria, sino a cada acto administrativo individualizado.

Hay que tener en cuenta y así lo recoje, el recurso, que el derecho a la intimidad y su correlativo, el derecho a la protección a la intimidad frente al procesamiento informático de los datos referentes a su vida privada, ciertamente no son derechos absolutos. Es amplia la doctrina del Tribunal Constitucional, según el cual los derechos fundamentales pueden ser objeto excepcionalmente de limitaciones, toda vez que el propio art. 103 CE obliga a los poderes públicos a actuar bajo los principios de eficiencia y eficacia, si bien siempre, bajo el imperio de la Ley, es lógico también que estos límites deban existir, pero igualmente es una obligación constitucional del legislador, al definir el campo de actuación de estas excepciones, evitar la total desnaturalización del derecho fundamental que pretende regular, en nuestro caso el de la autodeterminación informativa, valorando adecuadamente los derechos y obligaciones en colisión.

Y si la norma aprobada no pondera suficientemente estos conflictos, y sin el debido respaldo constitucional deja sin contenido el mandato de la Carta Magna, debe, en consecuencia, declararse inconstitucional.

La valoración de la inconstitucionalidad de las excepciones debe hacerse, en el caso del derecho a la libertad informática, en función de los criterios hermenéuticos que nos establece el Convenio del Consejo de Europa de 28 de enero de 1.981, dado que de acuerdo con el artículo 10.2 de la Constitución, los derechos y libertades han de interpretarse de conformidad con los Tratados y acuerdos internacionales sobre las mismas materias ratificadas por España.

Se analizan los artículos 5, 6, 8 y 9, del Convenio, para puntualizar que cada una de las excepciones allí apuntadas tienen un contenido determinado y enjuiciable; conceptos jurídicos que si bien no definen su total amplitud -algo que sólo podrán hacer los Tribunales-configuran de una forma objetiva sus respectivos ámbitos de actuación.

Partiendo de la aplicabilidad directa del contenido del Convenio y la necesidad de interpretar las excepciones previstas en el mismo de una manera literal y estricta, los arts. 6.1, 19.1, 22.1 y 22.2 de la Ley Orgánica, violando el artículo 18.4 de nuestra Carta Magna y lo previsto en el Convenio del Consejo de Europa de 28 de enero de 1.981, establecen un conjunto de limitaciones al contenido mínimo de este nuevo derecho fundamental que, en relación con los ficheros públicos, lo dejan sin contenido real. De tal manera que a pesar de la

recepción legal de unas aparentes facultades para actuar, en la práctica se crea un orden jurídico que hace imposible "que el ciudadano pueda saber quién, qué, cuándo y con qué motivo se sabe algo sobre él" por medios informáticos.

Y lo es porque la discrecionalidad de las excepciones que incorpora la ley, en caso de banco de datos públicos, es de tal intensidad que, en el conjunto de su articulado, el derecho fundamental es dificilmente recognoscible, desapareciendo toda idea de limitación al uso informático de datos personales que exige el mandato constitucional, lo que lleva a que el ciudadano se encuentre en situación de indefension absoluta, sin que la ley impugnada establezca limite alguno, frente a posibles intromisiones ilegítimas en su intimidad habiéndosele privado de toda capidad de obrar. Intromisión incluso mucho más peligrosa que la hipotética "patada en la puerta" aducida a efectos de ejemplificación con relación al alcance y previsible aplicación de determinados preceptos de la ley de seguridad ciudadana, porque a diferencia de la anterior, visible y palpable, la vulneración de la intimidad por medios informáticos no se ve, no resulta tangible, pero existe y puede acabar eliminando la vida privada frente al poder público, haciendo desaparecer la esfera más íntima de su personalidad.

El artículo 6 es uno de los que se impugna por inconstitucional, pues segun el apartado 2, en los términos en que está redactado, determina que no es necesario en ningún caso el consentimiento del interesado para cualquier tratamiento informático de sus datos personales si el fichero es de carácter público, es decir, creado por medio de una Administración Pública.

Lo que significa que dicho artículo, apartado 2, es manifiestamente inconstitucional al crear una potestad discrecional de grado máximo, que vacía de contenido todo posible límite al poder informático establecido en defensa de los derechos fundamentales -como es exigible, según la Constitución- a favor de cualquier ente público. Potestad discrecional de imposible encaje con el mandato constitucional de limitar el uso informático para garantizar el honor y la intimidad personal y familiar.

El consentimiento del afectado no sólo es necesario en la fase de creación del fichero sino tambien en el momento de la cesión a terceros pues el control mínimo de la utilización de los datos personales de cada uno no sólo debe abarcar al momento inicial de su creación sino igualmente a los posibles usos que de ellos pudiera realizarse.

El artículo 19 sólo crea límites a las cesiones de ficheros de una Administración Pública a otra, o de un ente público a un particular, pero no impide la

cesión de datos entre los distintos ficheros existentes en el seno de una misma persona jurídica pública.

Esta cesión de datos, dentro del seno de una misma organización, sin ninguna limitación previa, al haberse eliminado el consentimiento del afectado, permite crear ficheros susceptibles de abarcar a la totalidad de los aspectos que componen la identidad de la persona humana, lo cual es un peligro gravísimo para la libertad del hombre y la defensa de sus derechos.

Desde un punto de vista constitucional, no se puede aceptar, el hecho de que la Administración Pública, con carácter general y por todo ámbito competencial, pudiera crear cualquier tipo de base de datos personales, sin necesidad del consentimiento del afectado, así como ceder internamente los ficheros creados para ampliar los ya existentes dentro de una misma organización pública, sin limitación alguna, pues sólo podrán establecerse excepciones cuando ponderados los intereses en juego, valorados los peligros potenciales de una y otra opción, deba entenderse que es más grave para el orden constitucional informar al afectado o permitirle el acceso y rectificación, que negarle el uso de estas facultades.

El primero de los supuestos previstos en el apartado 1º y el supuesto recogido en el apartado 2º, del artículo 22, supone un grado de indeterminación no encuadrable,a nuestro juicio, dentro de la defensa de intereses públicos o privados definidos, concretos y enjuiciables. Y en la medida que la ausencia de parámetros que definan correctamente esas excepciones implican un vacío que permite el discrecional uso de las limitaciones enunciadas, ambos apartados deben entenderse inconstitucionales por violación del art. 18.4.

Hablar, como hace el art. 22, de funciones de control y verificación es hablar de actividad administrativa, lo que indirectamente equivaldría a decir que siempre que el ente público entendiese que puede existir un impedimento grave para el desarrollo de su actividad administrativa es posible limitar el derecho a informar al afectado en la recogida de datos.

Tal generalidad no puede en absoluto justificarse constitucionalmente, pues sería contraria al propio contenido del art. 18.4 al conceder un grado de discrecionalidad incompatible con el principio de seguridad jurídica y de interdicción de la arbitrariedad de los poderes públicos recogido en el artículo 9.3 de la Constitución.

El apartado 2º del art. 22 incorpora, a juicio de los recurrentes, una peligrosa inconcreción e indefinición. La determinación de lo que es interés públi-

co no es tarea fácil. Esta vaguedad e indeterminación puede dejar sin contenido el mandato constitucional no sólo del artículo 18.4, sino como antes hemos indicado, del principio de seguridad jurídica.

Se motiva igualmente las causas de inconstitucionalidad del art. 20.3 de la Ley 5/1992 por violación de los artículos 18.4 y 16 de la CE, al permitir la recogida y el almacenamiento informático de datos personales relativos a la ideología, religión o creencias, al origen racial, salud o vida sexual en contra del contenido de dicho precepto, siempre teniendo en cuenta lo previsto en el artº. 6º del Convenio del Consejo de Europa.

En terminología del Convenio, estos datos, denominados "datos sensibles", afectan al círculo más íntimo de la persona humana, la defensa de los derechos fundamentales de la misma exige incluso más garantías que las previstas para el resto de los supuestos, sin permiso del interesado, sin las debidas garantías; y así lo hace la Constitución. Desde el momento en que se pretendiera traspasar sin autorización ese último recinto cerrado de la personalidad de cada individuo, en que se inscriben los "datos sensibles", correríamos el riesgo de dañar gravemente, e incluso en ocasiones de forma irreparable, el propio derecho fundamental de la dignidad humana.

D) CONCLUSIONES

Como, se desprende de lo apuntado, los recursos de inconstitucionalidad planteados persiguen finalidades distintas:

El del Defensor del Pueblo y el Grupo Parlamentario Popular, una mayor garantía del ciudadano, al intentar: la inconstitucionalidad del art. 19.1 e impedir con ello la cesión de datos de carácter personal, por la administración, sin el consentimiento de su titular, por la inconstitucionalidad del art. 22 quieren limitar las excepciones de los derechos de los afectados a la información, acceso, rectificación y cancelación en relacion con sus datos personales en el ámbito de los ficheros de titularidad pública.

Los recursos de las instituciones catalanas, no se dirijen a defender los intereses de los ciudadanos sino, fundamentalmente, por no decir exclusivamente, a limitar la competencia de los órganos estatales para conseguir una mayor competencia de las Comunidades Autónomas, (en la creación, mantenimiento, control y sanciones sobre los ficheros públicos y privados...), en una palabra a obtener una mayor competencia en el reparto competencial entre el Estado y las Comunidades Autónomas.

Nos hemos limitado a sintetizar los argumentos alegados por los recurrentes, sin entrar, en si los artículos recurridos son o no inconstitucionales ya que será nuestro Tribunal Constitucional quien ha de decir la última palabra.

V.- El Rango Normativo de la Lortad

La LORTAD, como hemos apuntado, es una ley compleja tanto por la variedad de sus contenidos cuanto por la terminología específica que utiliza y que nace para dar cumplimiento al mandato expreso del art. 18.4 de la Constitución, así como de la obligación adquirida por la ratificación del Convenio para la Protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal.

Aunque el artículo 18.4 de la Constitución sólo habla "de la ley" está claro que al final del punto 8 de la exposición de motivos, la propia Ley, nos dice que con ella se "está estableciendo un nuevo y más consistente derecho a la privacidad de las personas", si a esto añadimos el emplazamiento del art. 18, dentro del capítulo segundo, "Derechos y libertades" y más concretamente dentro de la Sección Primera, "De los derechos fundamentales y de las libertades públicas" y ponemos éste en consonancia con el artículo 81 de la Constitución nos lleva inexcusablemente al desarrollo de derechos fundamentales, que no puede ser de otra forma que por medio de Ley Orgánica. Estamos por tanto ante una Ley Orgánica, pero no en toda su extensión, pues la Disposición Final tercera deslinda y concreta que parte de esta Ley no tendrá el carácter de Orgánica al establecer "Los artículos 18, 19, 23, 26, 27, 28, 29, 30, 31, los Títulos VI y VII, las disposiciones adicionales primera y segunda y la disposición final primera tienen carácter de Ley Ordinaria".

El Tribunal Constitucional en Sentencia 160/1987 mantiene el criterio de que la propia Ley Orgánica podrá determinar, como hace en este caso, cuáles de sus preceptos son propios de su normativa y cuáles los deja a la Ley Ordinaria.

El legislador es el que tiene que concretar los preceptos que tienen el carácter de Ley Orgánica, pero teniendo en cuenta que el art. 81.1 de la Constitución, al definir las materias propias de la Ley Orgánica, se refiere al "desarrollo de los derechos fundamentales y de las libertades públicas", que como hemos visto es precisamente la rúbrica utilizada para designar el conjunto de los artículos comprendidos en la sección primera del capítulo II.

Así pues, los derechos fundamentales y libertades públicas a que se refiere el art. 81.1.2 de la norma suprema son los comprendidos en la sección 1ª del Capítulo II, título I, de su texto -S-76/1983- exigiéndose, por tanto forma orgánica para las leyes que los desarrollen de modo directo en cuanto tales derechos -S. 67/1985- pero no cuando meramente les afecten o incidan en ellos, so pena de convertir a las Cortes en "constituyentes permanentes" con la proliferación de Leyes Orgánicas" -S. 6/1982 y 160/1987-, y esto es lo que hace la Ley Orgánica 5/192 de regulación del tratamiento automatizado de datos de carácter personal, que no sólo configura un nuevo derecho sino que también lo compagina con los demás derechos reconocidos en la Constitución.

Nos encontramos por tanto ante una Ley Orgánica o más correctamente ante "una ley parcialmente orgánica".

Por Ley Orgánica se regulan las reglas que contienen los grandes principios de la protección de datos, y las que configuran los derechos de las personas y sus límites, así como las que regulan el flujo transfronterizo de datos.

Como Ley ordinaria se regulan la parte que se refiere a los requisitos para la creación de ficheros, con excepciones, a la elaboración de códigos tipo, al estatuto y funciones de la Agencia de Protección de Datos, al régimen de infracciones y sanciones, en una palabra a las que son meramente organizativas y de funcionamiento.

VI.- Notas a la L.O.R.T.A.D.

Todos y cada uno de los títulos de la Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal son analizados, en profundidad, en esta publicación.

La exposicion de motivos y los titulos I, II y III son analizados por Miguel López Muñiz.

Al título III dedica un detenido estudio Guillermo Orozco.

Emilio del Peso y lo hace sobre los ficheros a que se refiere el título IV.

El título V sobre movimiento internacional de datos es analizado por Santiago Ripol Carulla.

Al título VI -Agencia de Proteccion de Datos-, dedican sus trabajos Manuel Heredero y Cinta Castillo.

El título VII dedicado a infracciones y sanciones lo analiza Carlos Romeo Casabona.

Si a los trabajos, anteriores, unimos los artículos, igualmente publicados en este número,de Antonio Perez Luño, Alfonso de Julios Campuzano, Miguel Ramos, Alvaro Sánchez Bravo, Stewart H. Dresner, María Lázpita Gurtubán, Jordi Bacaria, Ana Rosa González, Josep Jover i Padró, Vicente López-Ibor Mayor y Audilio Gonzales, nos encontramos con que todos los puntos fundamentales de la LORTAD van a ser tratados, en profundidad, en esta publicación, en la que no introduciremos, como era nuestro primitivo deseo, un artículo sobre un punto concreto que incidiría con alguno de los ántes mencionados y por el contrario nos limitaremos, como venimos haciendo, a unos conceptos generales y un resumen de los recursos de inconstitucionalidad, para continuar con un somero recorrido por la Ley, ateniéndonos, en lo posible, a la estructura de la misma, para intentar dar una visión general de la LORTAD.

A) ESTRUCTURA DE LA LEY

La LORTAD se ha estructurado, con una ámplia exposición de motivos, tres disposiciones adicionales, una disposición transitoria, una derogatoria, cuatro disposiciones finales y 48 artículos repartidos en los siguientes siete títulos:

Título I.- Disposiciones generales (arts. 1 a 3).

Título II.- Principios de protección de datos (arts.4 a ll).

Título III.- Derechos de las personas (arts.l2 a l7).

Título IV.- Disposiciones sectoriales -con dos capítulos, relativos a los ficheros de titularidad pública y privada- (arts. l8 a 3l).

Título V.- Movimiento internacional de datos (arts. 32 y 33).

Título VI.- Agencia de Protección de datos (arts. 34 a 4l).

Título VII.- Infracciones y sanciones (arts.42 a 48).

Como vemos al título IV, relativo a los ficheros, se le dedican l4 artículos, casi el 30% de la Ley, concretamente el 29,l66 %; le sigue con 8 artículos el título II -protección de datos- y VI -Agencia de Protección de Datos-; dedicando 7 artículos a las infracciones y sanciones, 6 a los derechos de las personas, 3 a las

Disposiciones generales, para ocupar el último lugar, en cuanto a artículos dedicados a ello, el Título V -movimiento internacional de datos,- con dos artículos sobre la materia.

El análisis, de la Ley española de protección de datos personales, o mejor dicho, las notas sobre la misma, la haremos, como hemos indicado, siguiendo su estructura, aunque pudieramos haberlo hecho partiendo del estudio de su finalidad, ambito de aplicación, conceptos básicos, obtención de los datos, el derecho de acceso, rectificación y cancelación, la creación de ficheros, las infracciones y sanciones, la autoridad de control, etc., si bien todos estos conceptos serán pieza clave de nuestras notas.

B) EXPOSICION DE MOTIVOS

La lentitud de los trabajos parlamentarios, que concluyeron con la publicacion de la Ley en el B.O.E del 3l de octubre de l992, y su entrada en vigor el 3l de enero de l.993, no fueron obstaculo para que en ella nos encontremos con una amplia exposición de motivos.

Lo más destacado es, por tanto, su amplitud, la discrepancia, en algunos casos, con la Ley y el intento excesivo de justificar o explicar algunos de los conceptos utilizados en el texto.

Según la exposición de motivos, la ley tiene su base en el mandato del artículo l8.4 de la Constitución.

Se desprende claramente la falta, en las Cortes Generales, de la "Comisión de estilo", que hubo en otros tiempos, pues ya en la propia exposición de motivos se utilizan palabras cuyo léxico es poco habitual e incluso en algunos casos con imprecisiones técnicas.

En el segundo párrafo del apartado primero de la exposicion de motivos se introduce un concepto "privacidad" que no aparece en todo el texto artículado de la Ley, intentando diferenciar este concepto con el de intimidad, diciendo que la privacidad constituye un conjunto más amplio, más global, cuyas fronteras estaban defendidas por el tiempo y el espacio. Uno y otro límite han desaparecido, hoy, ya que las modernas técnicas de comunicación permiten salvar sin dificultad el espacio y el tiempo.

Según hemos puesto de manifiesto, anteriormente, poco menos de la tercera parte de la ley gira en torno a los ficheros y eso ya queda plasmado en el apartado segundo de la exposición de motivos donde claramente aparece que

la Ley se nuclea en torno a los que convencionalmente se denominan "ficheros de datos", concibiendo los ficheros desde una perspectiva dinámica.

Se nos dice igualmente que la Ley se estructura en una parte general y otra especial. Que se recogen principios y definen derechos y garantías, para ya en ella hablarnos de datos sensibles, consentimiento o autodeterminación, excepciones, para matizarnos, en el apartado tercero, que los derechos de acceso a los datos, de rectificación y de cancelación, se constituyen como piezas centrales del sistema cautelar o preventivo instaurado por la Ley.

Según la exposicion de motivos en la transmisión internacional de datos se ha optado por exigir que el país de destino cuente en su ordenamiento con un sistema de protección equivalente al español.

En el apartado quinto de la exposición de motivos se quiere justificar la absoluta independencia de la Agencia de Protección de Datos, a quien se atribuye la aprobación, sin valor reglamentario, de las normas elaboradas por iniciativa de las asociaciones y organizaciónes pertinentes.

Como pone de manifiesto el apartado 7 la Ley no consagra nuevos tipos delictivos, y finaliza el apartado octavo justificando la necesidad de un periodo transitorio por la necesidad de ajustar la utilización de los ficheros existentes a las disposiciones legales.

C) DISPOSICIONES GENERALES

1) ***Objeto y finalidad.***

La Ley dedica los tres primeros artículos a las disposiciones generales, en las que se artícula el objeto, ambito de aplicación, así como definiciones de: datos de carácter personal; ficheros automatizados, tratamiento de datos, responsable del fichero y procedimiento de disociación.

El empleo del ordenador hace posible recopilar una amplia información sobre cada persona, reuniendo un conjunto de datos que aisladamente nada dicen, pero que al ser presentados en forma sistematizada, puedan dar lugar a una información que el afectado no se imagina ni le agradaría ver en poder de otros. Tengamos presente que un ordenador puede clasificar y relacionar rápidamente, por ejemplo, nuestros datos laborales, económicos, legales, salud, etc, construyendo un detallado perfil de cada individuo.

Precisamente peligra la intimidad cuando se relacionan entre sí archivos nominativos, pues la tecnología informática permite ahora, gracias a sus posi-

bilidades prácticamente ilimitadas de captar, almacenar, relacionar y transmitir los datos, reunir de forma personalizada, a partir de informaciones dispersas e, incluso anónimas, múltiples facetas de la vida de hombres y mujeres, que pueden ser utilizados por terceros y depararles perjuicios importantes.

Es importante, por tanto, cualquier dato, por insignificante que éste sea, ya que relacionado con otros puede poner en peligro la intimidad, pues como claramente pone de manifiesto el Tribunal Constitucional Federal aleman, en sentencia de 15 de diciembre de 1.983 ya no hay datos "sin interes" y asi señala:

"De este modo un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, ya no existe, bajo la elaboración automatizada de datos, ninguno "sin interés".

Como queda constancia las bases de datos nominativos son un peligro para la intimidad, no obstante, y si tenemos presente que en un sociedad moderna se hace imposible prescindir de los medios informáticos, sólo nos queda intentar desarrollar la más acabada protección legal posible y la LORTAD es un nuevo instrumento jurídico apto para proteger, según el artículo 1º, el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos, contra posibles atentados, excesos o errores provenientes de la utilización de medios automatizados.

En la exposición de motivos, ya se sienta tal principio, al recoger que la finalidad de la Ley es hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos. Como dice Santamaría Ibeas[5] se trata de asegurar que las garantías de los derechos fundamentales en general y del derecho a la intimidad en concreto no se vean modificados por la aparición de nuevas técnicas de comunicación, de modo que la estructura tradicional de los derechos fundamentales no sea alterada ni lo que es más importante, reducida respecto de lo que ha sido su normal desarrollo desde el siglo XVIII.

Coincidimos con el Profesor Vilariño[6] cuando dice en relación con la razón de ser de la Ley, el artículo 1º, al transcribir el texto del artículo 18.4 de la Constitución, confunde el mandato constitucional con la verdadera finalidad

- 5 SANTAMARIA IBEAS, Jose Javier: "La L.O.R.T.A.D.: Breve análisis de sus antecedentes", Actas del III Congreso Iberoamericano de Informática y Derecho, U.N.E.D. - Mérida.
- 6 VILARIÑO PINTOS, Eduardo: "La Ley de Regulación del Tratamiento Automatizado de Datos de Carácter Personal ante el Derecho Internacional", Generalidad de Cataluña, Barcelona 1993.

de las leyes sobre el tratamiento automatizado de datos personales, que no es la protección de datos personales, sino la protección de las personas en relación con el tratamiento automatizado de esos datos, como correctamente denomina el Convenio del Consejo de Europa. De ahí que no sea el honor o la intimidad lo que debe proteger estas leyes, sino el correcto uso y tratamiento de todos los datos de carácter personal, de los que sólo una parte, y pequeña, se referirán a la intimidad y al honor si se parte de una ajustada diferenciación de los distintos ámbitos a los que, en relación con las personas, hacen referencia los diversos datos.

La necesidad de la LORTAD y de regular el tratamiento informatizado de los datos personales, impuesta, como hemos reiterado varias veces, por mandato constitucional, dentro de las libertades fundamentales de los ciudadanos, viene determinada por las exigencias propias de un Estado de Derecho, como protección no sólo de una intimidad, en cuanto derecho esencial integrador de la personalidad, sino también de los derechos y libertades públicas en sentido amplio, frente a los excesos y abusos que conllevaría un poder absoluto e incontrolado de la Administración y otras entidades públicas o privadas sobre esos datos, poniendo en peligro la propia identidad personal.

En esta misma linea está el Profesor Murillo de la Cueva[7] al manifestar que el conjunto de competencias normativas del artículo l8 de la Constitución tiene como punto de referencia a la persona y a aquellas manifestaciones de la misma que le son más propias. Por tanto, no parece descabellado identificar en la defensa de la personalidad -como clave genérica- el bien protegido. Facilitan esta conclusión no sólo las menciones explícitas a expresiones de ella como el honor o la intimidad, sino tambien la evidente conexión que así existe con lo que se señala en el artículo l0.1 de la Constitución sobre la dignidad de la persona y el libre desarrollo de la personalidad. A partir de aquí, y considerando, además, que el apartado 2° de este mismo artículo l0 remite a los acuerdos internacionales ratificados por España para la interpretación de las normas relativas a los derechos fundamentales y a las libertades -o sea, a la vista del convenio europeo de 28 de enero de l.98l- no parece que existan mayores dificultades que concluir que el objeto de protección es esa dimensión de la personalidad que hemos llamado antes intimidad, o mejor, autodeterminación informativa, y que comporta para el particular el control sustancial sobre la utilización de sus datos personales.

■ 7 MURILLO DE LA CUEVA, Pablo Lucas: "La Protección de los Datos Personales ante el uso de la Informática", Revista de la Facultad de Derecho de la Universidad Complutense de Madrid, Núm. l5 pág. 6l4.

En definitiva el bien a proteger comprende y supera el de la estricta intimidad, dando pie a la configuración de un nuevo derecho fundamental: el derecho de la **autodeterminación informativa**, pues no se trata de prohibir el uso de la informática, pero sí de encaminarlo dentro de unos cauces idóneos para evitar sus peligros, ya que estamos ante la exigencia de ampliar la protección de ciertos derechos en el ámbito en que opera la informática.

Siguiendo a la LORTAD, y como hemos dicho anteriormente, podemos concluir que de acuerdo con lo dispuesto en el artículo l° de la Ley, ésta tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad y el pleno ejercicio de los derechos de las personas.

Al comparar el artículo l° de la LORTAD con el artículo 1° del Convenio de Estrasburgo, ambos preceptos referidos al objeto y fin, vemos que este último puntualiza que el fin del mismo no es el de "limitar" sino el de "garantizar" a cualquier persona física, 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.

2) *Ambito de la Aplicación*

Aparece definido en el artículo 2 de la Ley, que hace una acertada declaración general al extender el alcance de la Ley tanto a los ficheros de titularidad pública como de titularidad privada, así como al uso no automatizado de los datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado.

Del parrafo l° del artículo 2 se desprende claramente que "la presente Ley será de aplicación a los datos de carácter personal ", es decir se excluye la protección de las personas jurídicas y con ello se sigue la opción mayoritaria de no incluir a las personas jurídicas, quiza por influencia del proyecto de directiva comunitaria que acoge idéntica solución restrictiva, siguiendo el mismo proceso que la Ley francesa y en contraposición a la legislación de Austria, Dinamarca, Luxemburgo y Noruega que incluyen en la protección de dicha normativa también a las personas jurídicas.

Siguiendo a Piñoll i Rull y Estadella Yuste[8], cabe manifestar, que por ahora el proyecto de directiva de la CEE sobre el tema de nuestro análisis, a

■ 8 LLUIS PIÑOL I RULL, Joan y ESTADELLA YUSTE, Olga: "La Regulación de la Transmisión Internacional de Datos en la L.O. 5/1992 de 29 de octubre", Generalitat de Catalunya 1993.

pesar de la recomendación a favor de la inclusión en su texto de las personas jurídicas hecha en el informe Bayerl, no ha recogido tal posibilidad, probablemente ante el temor, subyacente en las directrices de la OCDE, de que tal extensión de la protección de datos a sociedades fuese considerada por Estados Unidos, en especial, como una forma restringida de libre flujo de la información y la libre competencia en los servicios a nivel mundial y, además con un interés jurídico protegido mucho menos claro que en el caso de las personas físicas.

La disposicion final segunda permite al Gobierno, previo informe del Director de la Agencia de Protección de Datos,extender la aplicación de la presente Ley, con las modificaciones y adaptaciones que fuesen necesarias, a los ficheros que contengan datos almacenados en forma convencional y que no hayan sido sometidos todavía o no estén destinados a ser sometidos a tratamiento automatizado.

Tras estas declaraciones de principios, que aparenta que la Ley se aplica al tratamiento de datos de personas físicas que se realicen en el ámbito público o privado, afectando a cualquier tipo de ficheros,nos encontramos,en el número 2 del artículo 2º de la Ley, con tal cúmulo de excepciones y de regímenes específicos, no siempre justificables, que podrían ser fácil excusa para su inaplicación y sobre todo para poder dejar a la Ley vacía de contenido, al unirse estas excepciones a otras numerosas que aparecen a lo largo de la Ley y que han sido la principal causa de los recursos de inconstitucionalidad planteados a la misma.

Hay dos tipos de excepciones: las contenidas en la disposición adicional primera y las contenidas en el número dos del artículo 2, que establece la Ley, no será de aplicación, además de a los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su públicidad con carácter general; a los ficheros mantenidos por personas físicas con fines exclusivamente personales; a los de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales; a los ficheros de información jurídica accesibles al público, cuando se limite a reproducir disposiciones o resoluciones judiciales, publicadas en periódicos o repertorios oficiales; a los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones o comunidades religiosas en cuanto los datos se refieran a sus asociaciones o miembros y ex miembros, aunque en este caso la cesión de los datos quedara sometida a Ley.

Si a lo anterior, no le es aplicable la Ley en su integridad, no ocurre lo mismo con lo recogido en la disposición adicional primera que excluye, única-

mente, la aplicación de los títulos VI y VII de la Ley, a los ficheros automatizados de los que sean titulares las Cortes Generales, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo General del Poder Judicial y el Tribunal Constitucional.

En el párrafo tercero, el artículo 2 hace una nueva exclusión del alcance de la Ley al determinar que se regirán por sus disposiciones específicas: los ficheros regulados por la legislación de régimen electoral; los sometidos a normas sobre materias clasificadas; los derivados del Registro Civil y del Registro Central de Penados y Rebeldes; los que sirvan a fines exclusivamente estadísticos al amparo de la Ley de la función estadística pública; los ficheros cuyo objetivo sean los datos de los informes personales bajo la regulación de la Ley del régimen del personal militar profesional.

3) ***Definiciones***

A los efectos de la presente Ley, dice el artículo 3, lo que deberá entenderse por datos de carácter personal, ficheros automatizados, tratamiento de datos, responsable del fichero, afectado y procedimiento de disociación.

Se echa de menos, en este artículo, la definición de las diferentes categorías de datos de carácter personal; lo que debe entenderse por titularidad pública o titularidad privada, cesión de datos, bloqueo de datos, datos accesibles al público, datos de carácter personal, identificación del afectado, etc.

D) PRINCIPIOS DE PROTECCION DE DATOS

A los principios de protección de datos se dedica el Titulo II de la Ley, que comprende desde el artículo 4 al 11 inclusive y en los que se regula la calidad de datos, información en la recogida de datos, consentimiento, datos especialmente protegidos, dastos relativos a la salud, seguridad de los datos , deber de secreto y cesión de datos

1) ***Calidad de los datos***

El artículo 4, con el que comienza el título II, establece una serie de principios o garantías que podemos sintetizar así: adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido, no pudiendo usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos; también deberan ser exactos y puestos al día, de lo contrario deberan ser cancelados, rectificados, completados o sustituidos; se alamacenaran, los datos, de forma que permita el ejerci-

cio del derecho de acceso por parte del afectado; se prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos; los datos de caracter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual, hubieren sido recabados.

2) *Recogida de datos*

El derecho de información en la recogida de datos es tratado en el artículo 5, que establece que los afectados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: de la finalidad de la recogida de éstos y de los destinatarios de la información; del carácter obligatorio o facultativo de su respuesta , así como de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; los derechos que le asisten respecto al acceso, rectificación y cancelación; la identidad y dirección del responsable del fichero.

3) *El Consentimiento Afectado*

Según el art.6, salvo que la Ley disponga otra cosa, el tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado.Sin embargo, el apartado segundo de dicho artículo contiene varias excepciones ordinarias: al disponer que no será preciso el consentimiento cuando los datos de caracter personal se recojan de fuentes accesibles al público, o cuando se refieran a personas vinculadas por una relación negocial laboral, administrativa o contractual. y sean necesarias para el mantenimiento de las relaciones o para el cumplimiento de las obligaciones, y una excepción de gran amplitud y generalidad, al disponer que no será preciso el consentimiento cuando los datos se recojan "para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias". Con esta excepción, conforme al Profesor Tasende Calvo[9], prácticamente se elimina el consentimiento del afectado como requisito previo al tratamiento automatizado de datos personales por la Administración, a cuyo discrecional y exclusivo criterio se encomienda la recogida de tales datos, sin que la ausencia de voluntad del interesado sea suplida por un inmediato control o intervención judicial o, cuando menos, de la Agencia de Protección de Datos.

■ 9 TASENDE CALVO, Julio J.: "Notas al Proyecto de Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal", Poder Judicial, septiembre 1991.

Desgraciadamente este artículo 6.2 ha tomado como base el artículo 8 de la anterior propuesta de Directiva, suprimido en la actual, y que, siguiendo al Profesor Vilariño, en cualquier caso, se trata de una disposicion de discutible conformidad con el Convenio del Consejo de Europa; pero además, el art. 6.2 amplia los supuestos de ese extinto artículo 8. En todo caso, por esta via de exclusión del consentimiento se hace inaplicable el artículo 5, sobre la obligación de informar al afectado y, por tanto, se producirá el tratamiento de los datos personales sin conocimiento del interesado.

Como hemos puesto de manifiesto anteriormente el artículo 6.2 ha sido objeto de recurso de inconstitucionalidad por parte del Grupo Parlamentario Popular del Congreso de los Diputados.

La Ley nada dice, en este artículo ni en las disposiciones adicionales o transitorias, sobre los ficheros que ya esten funcionando en el momento de entrar en vigor esta norma, aunque, lo lógico, sería que el responsable del fichero informara y solicitara el consentimiento a todas las personas que figuren en ellos, toda vez que el artículo 6.1 enuncia la regla capital en materia de protección de datos, el consentimiento del afectado, que de otra forma se vería violada, e impediría,sobre lo ya existente, la autodeterminación o autodisposición sobre la información que le atañe.

No cabe consentimiento concedido con caracter general sino que el mismo ha de ser concedido caso por caso.

La exigencia fundamental del consentimiento del afectado para el tratamiento automatizado de datos de carácter personal, solo podrá ser revocado, conforme al número tercero del artículo 6, cuando exista causa justificada y sin efectos retroactivos. El consentimiento para la cesión de datos de carácter personal tiene también un carácter revocable (art.11.4).

Como hemos dicho, el art. 6.1, enuncia la regla capital en materia de protección de datos: el consentimiento y por ello este aparece en varios preceptos de la ley y que en algunos casos ha de ser necesariamente expreso y prestarse por escrito (arts.7.2 y 3), de ahí que los derechos de información, acceso, rectificación y cancelación, así como los demás que la LORTAD contempla en su título III, no sean, siguiendo a Lucas Murillo de la Cueva, sino una manifestación específica, una proyección concreta, de este elemento capital, del mismo modo que lo son las facultades que los artículos 11.1 y 3 , l9.3, 28.1 y 2, 29.2, 30.l reconocen a la persona a la que se refieren los datos.

El legislador, para asegurar una mayor protección, ha acotado claramente el marco en el que ese consentimiento se presta en cada ocasión, poniendo,

igualmente, los medios necesarios para asegurar que el uso que de ellos se hace concuerdan con los términos en que expresó su voluntad.

Podemos concluir,con el consentimiento del afectado, diciendo que ésta es la piedra angular a partir de la que se construye el sistema de protección de datos personales frente al uso de la informática.

4) *Datos especialmente protegidos*

Bajo el epígrafe de datos especialmente protegidos encuadra el artículo 7, algunos datos de carácter personal, que se ha convenido en denominar "**datos sensibles**", expresión nueva en nuestro lenguaje jurídico, y a los que la LORTAD quiere proteger de una manera especial.

Se incluyen entre ellos los que se refieren a la **ideología, religión** o **creencias**, así como los datos de carácter personal que hagan referencia al **origen racial**, a la **salud** y a la **vida sexual**. El último párrafo de citado artículo incluye también a los datos de carácter personal relativos a la comisión de infracciones penales o administrativas, dentro de los datos especialmente protegidos.

La Ley no da la misma protección a todos estos datos y siguiendo a Murillo de la Cueva, distinguiremos, de acuerdo con las previsiones de la Ley, tres categorías:

En la primera figuran los datos sobre la ideología, religión o creencias. Las especialidades que revisten los mecanismos ideados para protegerlos consisten en la exigencia de que el **consentimiento se exprese por escrito y de manera explícita** (art.7.2). Además será necesario que, cuando se recabe la autorización, se advierta especialmente al interesado de su derecho a no prestarlo, ya que estos aspectos de la personalidad gozan de amparo constitucional específico, al establecer el artículo l6.2 de la CE que "nadie podrá ser obligado a declarar sobre su ideología, religión o creencias".

En la segunda se hallan los datos que afectan al origen racial, la salud y la vida sexual. En este caso, el artículo 7.3 establece, como ya hemos dicho anteriormente, que sólo podrán ser recogidos, tratados automáticamente y cedidos cuando el afectado otorgue su consentimiento expreso o en los supuestos en que, por razones de interés general, una ley así lo disponga. La excepción que permite prescindir, en materia tan delicada, de la voluntad del afectado está justificada, ya que parece suficiente garantía sustituirla por una habilitación del legislador fundada en razones de interés general, Ley que por otra parte

tendrá el carácter de Orgánica, dado el carácter de Ley Orgánica del artículo 7 y por la naturaleza de información que estamos contemplando.

Como hemos indicado, en el último párrafo del artículo 7, nos encontramos con una tercera categoría, la constituida por los datos personales referentes a infracciones penales o administrativas, los cuales solamente podrá figurar en los ficheros automatizados de las Administraciones Públicas siempre que éstas sean competentes en la materia y que tengan lugar en los supuestos, expresamente, previstos, en sus normas reguladoras.

El legislador, en su deseo de disuadir en el tratamiento indebido de estos datos, al tipificar, en el art. 43, las infracciones, califica de muy graves "recabar y tratar de forma automatizada los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar de forma automatizada los datos referidos al apartado 3 del artículo 7 cuando no lo disponga una Ley o el afectado no haya consentido expresamente o violentar la prohibición contenida en el apartado 4 del artículo 7" (artículo 43.4.c) e igualmente en el artículo 44 al determinar los tipos de sanciones, expresa, en su número 4, que "la cuantía de las sanciones se graduará atendido a la naturaleza de los derechos personales afectados..."

5) ***Datos relativos a la Salud***

El artículo 23 de la Ley l4/l.986, de 25 de abril, General de Sanidad, autoriza, a la Administración Sanitaria, de acuerdo con sus competencias, para crear los Registros y elaborar los análisis de información necesaria para el conocimiento de las distintas situaciones de las que pueden derivarse acciones de intervención de la antoridad sanitaria.

Según el artículo 6l de dicha Ley el historial clínico sanitario, estará a disposición de los enfermos y de los facultativos que directamente estén implicados en el diagnóstico y tratamiento del enfermo, debiendo quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica.

Por el artículo 8 de la LORTAD se faculta a las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes para proceder al tratamiento automatizado de los datos de carácter personal relativo a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, si bien, en la cesión de los mismos, no será preciso el consentimiento del afectado, conforme determina el apartado 2 letra f) del artículo ll, cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para

solucionar una urgencia que requiera acceder a un fichero automatizado o para realizar los estudios epidemiológicos necesarios para orientar con mayor eficacia la prevención de los riesgos para la salud, así como la planificación y evaluación sanitaria.

6) *Cesión de Datos*

El artículo 11, último del título II, se dedica a la cesión de datos, precedido de los artículos relativos a la seguridad de los datos y el deber de secreto, de los que posteriormente haremos mención.

En principio, y conforme al párrafo 1 del artículo 11,la cesión de datos personales solamente puede producirse para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

El consentimiento del afectado es básico para la cesión de datos. Se le ha de solicitar en términos concretos e informándole quién es el cesionario y la finalidad que se pretende con la cesión, de lo contrario sera nulo el consentimiento prestado.

Le es aplicable, a la cesión de datos, todo lo anteriormente, apuntado sobre el consentimiento.

Con la salvedad de los datos sensibles (art.7.3) y de los relativos a la salud (art.ll.7), que requieren un régimen distinto para ser cedidos, la regulación o mejor dicho las excepciones contenidas en el número 2 del artículo ll nos vuelven a poner de manifiesto que dicho artículo queda seriamente devaluado, al establecer que no será preciso el consentimiento, cuando una ley prevea otra cosa, o sean datos recogidos de fuentes accesibles al público; cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros. Tampoco requerirá el consentimiento las cesiones de datos que tengan por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales, en el ejercicio de las funciones que tienen atribuidas.

Según este artículo, no será necesario el consentimiento del afectado, cuando la cesión se produzca entre las Administraciones Públicas en los supuestos previstos en el artículo l9, precepto sometido a recurso de inconstitucionalidad ante el temor de que los datos cedidos sean utilizados para fines diferentes de los que determinaron su recogida.

E) DERECHOS DE LAS PERSONAS

Los aspectos principales de la posición de los ciudadanos a quienes pertenecen los datos a tratar informáticamente, se hallan recogidos en el Título II y III de la LORTAD.

Los preceptos del Título II, como se desprende del apartado anterior, se dedicán más bien a definir el marco en el que han de moverse quienes deseen operar con datos de carácter personal y la forma en que pueden recogerlos, tratarlos, conservarlos y cederlos, mientras que **el Título III**, al que vamos a dedicar este apartado, **constituye el núcleo del sistema de garantías de la Ley** y se centra en los derechos de las personas a información, acceso, rectificación, cancelación e indemnización y se encuentra regulado en los artículos 12 a 17, ambos inclusive, de la LORTAD.

1) ***Derecho de la Información***

En nuestra época el poder que confieren las modernas tecnologías a los centros recolectores de información exceden los límites de lo imaginable.

Nuestros legisladores, conscientes de tal poder y su repercusión, introducen en la Ley el artículo 13 que faculta a que "Cualquier persona pueda conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de ficheros automatizados de datos de carácter personal, su finalidad y la identidad del responsable del fichero."

Este derecho de información no es el adecuado, puesto que lo único que se concede es la facultad de conocer que ficheros existen, pero no en cuales se encuentra registrado el interesado y los datos que del mismo se contienen en cada uno. Este principio de información queda en la Ley sustituido, en este sentido, por el derecho de acceso, confundiendo ambos.

El supuesto contemplado en el artículo 13, va destinado a facilitar información sobre la existencia de ficheros automatizados de datos de carácter personal y sus finalidades, distinto al derecho a la información en la recogida de datos que reconoce el artículo 5 de la Ley.

Con el fin de facilitar este derecho se dispone, igualmente, que "El Registro General será de consulta pública y gratuita".

Poniendo en consonancia los dos preceptos citados nos encontramos que hay un derecho de información, previo a la recogida de los datos personales,

acerca de la finalidad y el destinatario de la información que se recaba, así como de los derechos que, en general corresponden al afectado como consecuencia de la obtención de tales datos, y otro derecho de información que nos permitirá conocer, con posterioridad, la existencia de ficheros automatizados de datos de carácter personal.

2) *Derecho de acceso*

El derecho de acceso, recogido en el artículo l4 de la Ley, otorga al afectado la facultad de solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados, tiene incluso plasmación constitucional, pues esta facultad aparece reconocida no con el rango de derecho fundamental, pero sí como derivación del derecho a recibir libre información en el artículo l05.b de la Constitución.

Por medio del derecho de acceso la persona tiene la facultad de conocer la información que le concierne y controlarla mediante el derecho de rectificación y cancelación.

Podemos considerar el derecho de acceso como el **eje del sistema de garantías arbitrado por la Ley**, ya que faculta a su titular o el legitimado para ello para exigir el conocimiento preciso de los datos de carácter personal que se incluyan en un fichero automatizado.

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 especiales (art.l4.2).

El derecho de acceso se ve limitado, en el tiempo, pues, conforme al apartado 3 del artículo l4 , este derecho se puede ejercitar en plazos no inferiores a doce meses, salvo que el afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Las **excepciones**, a este principio, son generosas y se consagran, básicamente, en los artículos 2l y 22, para ficheros de titularidad pública (Fuerzas y Cuerpos de Seguridad del Estado, Hacienda Pública...), cuyo acceso queda indeterminado, mientras el acceso cobra plena efectividad en el campo de los ficheros de titularidad privada.

La ley, en su artículo l6, nos indica que el procedimiento para ejercitar el derecho de acceso, así como el de rectificación y cancelación serán establecidos

reglamentariamente, esperemos que sean desarrolladas cuidadosamente, si bien consideramos debería regularse por Ley con el fin de ofrecer mayores garantías.

El artículo 22.2, establece que si el órgano administrativo dicta resolucion negativa instruirá al afectado del derecho que le asiste de dirigirse a la Agencia de Protección de Datos, o en su caso, del órgano equivalente de las Comunidades Autónomas, para terminar, si fuese necesario, en los Tribunales de Justicia.

Por la rectificación o cancelación de los datos de carácter personal inexactos no se exigirá contraprestación alguna, según el art.l6, que por otra parte no dice nada, sobre la gratuidad o no, del derecho de acceso.

3) *Derecho de rectificación y cancelación*

El derecho de rectificación y cancelación, unidos a los derechos de información y de acceso constituyen el **núcleo del sistema de garantías** previstos en la Ley y recogidos en los artículos l2 a l7,derechos a los que la exposición de motivos quiere destacar cuando dice: "los derechos de acceso a los datos, de rectificación y de cancelación, se constituyen como piezas centrales del sistema cautelar o preventivo instaurado en la Ley".

El artículo l5 sólo prevé que, cuando resulten inexactos o incompletos, los datos de carácter personal, serán rectificados y cancelados en su caso, pero se deja para **su regulación reglamentaria el procedimiento** para ejercitar el derecho de acceso, rectificación y cancelación en su caso, así como el plazo para que el responsable del fichero tenga la obligación de llevarlo a efecto.

Del párrafo precedente parece deducirse que siempre que haya un dato inexacto éste deberá cancelarse, de oficio o a instancia de parte, pero no hay que salir del mismo artículo para encontrarnos con que "La cancelación no procede cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando exista una obligación de conservar los datos", en el primer caso, supone, una sustitución inaceptable de la voluntad del propio interesado, el único a quien corresponde decir sobre lo que entiende que le perjudica y en los otros supuestos ¿es correcto mantener unos datos inexactos?.

Siguiendo a Velazquez Bautista[10] diremos que la actualización de la información es una de las obligaciones del creador o gestor de la base de datos, for-

■ 10 VELAZQUEZ BAUTISTA, Rafael: "Protección Jurídica de Datos Personales Automatizados", COLEX, Madrid l993.

ma parte de su trabajo, se halla directamente relacionado con la calidad del fichero, deberá cumplirse de oficio. Aunque esto no es óbice para que la actualización de los datos se plantee a partir del ejercicio del Derecho de acceso.

La rectificación, aunque pueda entenderse como una forma de actualizar los datos, no hay que considerarla como una actividad equivalente. Pues, mientras la rectificación presupone la existencia de unos datos erróneos, la actualización es una puesta al día de éstos, no porque los anteriores fueran incorrectos o erróneos, sino por que se han quedado desfasados.

Así, en el caso de rectificación sustituimos datos erróneos por información cierta o sin error, mientras en la actualización no hay por que sustituir información pues la misma no era errónea, sino que se ha quedado desactualizada. Según esto, quedan registrados sin modificarse los datos anteriores mientras se añaden unos datos nuevos gracias a los cuales se pone al día la información.

El derecho de rectificación aparece ya recogido en el artículo 8 del Convenio 81 del Consejo de Europa, así como en el art. 16 de la propuesta de Directiva Comunitaria, en forma similar al art. 15 de la LORTAD. De todos ellos se deduce que la posibilidad de que se rectifiquen los datos forma parte del mínimo necesario que deben contener las leyes de protección de datos, asimismo supone una consecuencia lógica del ejercicio del Derecho de acceso pudiendo afirmarse, que es una de sus finalidades

La rectificación y cancelación de los datos es una obligación que tienen los titulares de bases de datos, cuyo incumplimiento supone una infracción de la norma para la protección de datos, incluida entre las infracciones graves, en el art. 43.3.f) de la Ley y sancionadas conforme al art. 44.3 con multa de 10.000.001 a 50.000.000 de pesetas, más la indemnización que corresponda por la reclamación de daños y perjuicios que se pudiese exigir, ante los órganos de la jurisdicción ordinaria, si los ficheros fuesen de titularidad privada, en base al artículo 1902 del Código Civil y 17.3 de la LORTAD, por los causados como consecuencia del incumplimiento de lo dispuesto en la presente Ley. Si los ficheros fuesen de titularidad pública la via será la contencioso-administrativa.

Si los datos no fuesen pertinentes o adecuados a la finalidad que originó su registro, o pertenecen a la esfera privada del sujeto en tal grado que éste no desea que se registren, y no viene obligado a ello, o hubiese revocado su autorización para que sean incorporados al fichero, podrá, si no se hubiese hecho de oficio, ejercitar su derecho de cancelación exigiendo se borren o bloqueen tales datos.

Igualmente deberán ser cancelados los datos de carácter personal cuando finalice su periodo de vida o como dice el art.4 "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". La extensión de la duración guarda, conforme al núm. 5 del art. 15, relación con el fin para el que se obtuvieron, así como con lo que dispongan las disposiciones legales. Una serie de informaciones sobre las personas seguirán vivas incluso después del fallecimiento: ejemplo las inscripciones de nacimiento, matrimonio y defunción del Registro Civil, otras, del mundo empresarial y por mandato del art. 45 del Código de Comercio, deberán conservarse durante cinco años, en otros su duración podra ser fijada a priori y en otros no, pero en todos casos procede su cancelación.

Tema polémico está siendo la expresion "cancelar", pues para unos significa borrar, para otros anular, hacer ilegibles, destruir, dejar irreconocible, dejar nulos, etc, sería conveniente definir, a efectos de la presente Ley, qué se entiende por cancelar.

Otro tema conflictivo puede ser la rectificación o cancelación de los datos cedidos al extranjero, por la dificultad que, en algunos casos, puede entrañar hacer realidad tal derecho.

Las actuaciones contrarias a la presente Ley pueden ser objeto de reclamación, por los afectados, ante la Agencia de Protección de Datos y contra las resoluciones de éstas procederá recurso contencioso-administrativo (art. 17).

Para concluir, con el Título III, diremos que es clave en esta Ley, el derecho de las personas a acceder a los datos poseidos sobre ellos y controlar su posible divulgación.

Se trata por tanto de que la persona conozca y disponga de posibilidades reales de acceder a las informaciones que sobre ellos obran en manos de terceros, y se encuentran archivadas en bancos de datos. El consentimiento y acceso a la información es una garantía indispensable que debe reconocerse y tratarse jurídicamente (lo que se denomina como "habeas data", por analogía, a lo que significa respecto a la libertad personal el "habeas corpus", en este caso sería el derecho de acceder y conocer los datos referentes a uno mismo).

4) *Procedimiento*

Junto al acceso, el individuo debe controlar la calidad de los datos almacenados en ficheros electrónicos, a fin de poder, en su caso, rectificar o cance-

lar los datos inexactos o indebidamente procesados, al igual que debe disponer sobre su transmisión.

Para la efectividad de lo anterior hace falta un procedimiento que la Ley pospone a una decisión reglamentaria, no sólo del procedimiento para ejercitar el derecho de acceso, rectificación o cancelación, sino tambien, para las reclamaciones ante la Agencia de Protección de Datos.

Siguiendo a la Profesora Gayo Santa Cecilia[11], en cuanto al tratamiento específico que la LORTAD contiene en relación con la protección de los derechos de información, acceso, rectificación y cancelación, parece claramente insuficiente, no sólo por dejar en manos de la Agencia de Protección de datos, un órgano administrativo, la competencia para conocer y resolver las reclamaciones, pues consideramos que quizas un órgano judicial podría haber resultado más eficaz para resolver los posibles conflictos de intereses que surjan, más aun cuando la actuación ante la que se pretende reclamar ha sido realizada por la propia Administración pública; sino sobre todo por no concretar un procedimiento específico para su resolución.

Con todo se ha introducido una posible intervención de los órganos jurisdiccionales al hacer referencia el artículo 17.2 a la hipotética procedencia de un Recurso Contencioso-Administrativo contra las resoluciones de la Agencia de Protección de Datos, si bien surge la duda acerca de a qué tipo de Recurso Contencioso-Administrativo se está haciendo referencia, si al contenido en la Ley Reguladora de la Jurisdicción Contencioso-Administrativo o al regulado en la Ley 62/1.978 de 26 de diciembre de protección jurisdiccional de los dedrechos fundamentales de las personas, ya que, en el caso de que dicho recurso haya de tramitarse por la via contencioso-administrativa, la obtención de una resolución definitiva podría prolongarse excesivamente, lo que nuevamente supondría un menoscabo de los derechos y libertades de los ciudadanos.

El mismo resultado se produce en relación al Derecho a ser indemnizado del art. 17.3, tanto por la existencia de una duplicidad de regulaciones según se trate de ejercitarlo ante las Administraciones Públicas o ante sujetos privados, como por la elección de los órganos de la jurisdicción ordinaria como vía de salvaguarda de los derechos en el segundo de los supuestos, puesto que los

■ 11 GAYO SANTA CECILIA, Mª. Eugenia: "Garantías del ciudadano ante la L.O.R.T.A.D.: Posibles Vías de Defensa y Protección de sus Derechos Fundamentales", U.N.E.D. - Mérida, Actas III Congreso Iberoamericano de Informática y Derecho".

procedimientos que se pueden instar ante dicha jurisdicción son largos y complejos, lo que podría llegar a desvirtuar la finalidad protectora que se pretende.

F) LOS FICHEROS

La LORTAD, después de sentar los que ella llama principios y derechos de las personas en sus Títulos II y III, respectivamente, dedica el Título IV a lo que define como "disposiciones sectoriales", con dos capítulos, el primero de ellos, con cinco artículos del l8 al 22, dedicado a los ficheros de titularidad pública y el segundo, con nueve artículos del 23 al 3l, dedicado a los ficheros de titularidad privada

Conforme hemos apuntado, con anterioridad, la propia exposición de motivos nos indica que la Ley se nuclea en torno a los que convencionalmente se denominan "ficheros de datos", a tal efecto la Ley introduce el concepto de tratamiento de datos, concibiendo los ficheros desde una perspectiva dinámica, dicho en otros términos, no los entiende sólo como un mero depósito de datos, sino también, y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el perfil personal al que antes se hizo referencia.

En las disposiciones generales se dedica el artículo 3 a una serie de definiciones y entre ellas el apartado b) nos lo hace del fichero automatizado como: "Todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuese la forma o modalidad de su creación, almacenamiento, organización y acceso".

El concepto informático de fichero no se corresponde con el concepto jurídico, por lo que a efectos de notificación, toda una base de datos (definida en el artículo 12 de la Ley de Propiedad Intelectual, como la sistematización y/o recopilación de datos), compuesta por múltiples ficheros informáticos, puede ser tratada como un único fichero jurídico.

Si acudimos a los artículos 9 y l0, relativos al secreto profesional y seguridad de los datos, donde se habla del responsable del fichero automatizado, sin distinción de público o privado, podría llevarnos a la conclusión de que las normas contenida en esta Ley rigen por igual para todos, cualquiera que sea su naturaleza. El análisis del presente título nos pone de manifiesto que esto no es así, pues no sólo se ha definido un régimen jurídico distinto para unos y otros, sino que, respecto a los ficheros de titularidad pública, se ha introduci-

do, en casos señalados, notorias restricciones al ejercicio de los derechos de información, acceso, rectificación y cancelación.

1) *Ficheros de Titularidad Pública*

A ellos se dedica, como ya hemos indicado, el Capítulo Primero, del Título IV en sus artículos l8 a 22, ambos inclusive, y comienza diciéndonos que su creación, modificación o supresión de los ficheros automatizados de las Administraciónes Públicas sólo podran hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o diario oficial correspondiente y en la que deberá indicar: la finalidad, las personas sobre las que se pretende obtener los datos, el procedimiento de recogida, la estructura básica, las cesiones, los responsables del fichero...

Para dar cumplimento al artículo 18 los órganos de gobierno de los Poderes e Instituciones públicas, en el ejercicio de sus competenecias y en el ámbito de su propia organización deberán adoptar un acuerdo -de indudable matíz reglamentario- por el que se decida crear, modificar, o estinguir el oportuno fichero automatizado de datos, con las especificaciones del citado artículo 18.

Las excepciones, hacen pensar que existen limitaciones en el ejercicio de los derechos reconocidos a los ciudadanos, cuando se trata de ficheros de titularidad pública, pues ellas permiten la cesión de datos de carácter personal, en determinadas circunstancias, entre Administraciones Públicas, e incluso la recogida y tratamiento automatizado por las Fuerzas y Cuerpos de Seguridad, sin consentimiento de las personas afectadas, de los datos a que hacen referencia los apartados 2 y 3 del artículo 7, esto es, los que se han dado en llamar "datos sensibles".

Algunas de las excepciones contenidas en los artículos 19, 20 y 22 suponen un grado de indeterminación y un vacío que permite el discrecional uso de las limitaciones enunciadas en la Ley y que han dado lugar a que, tanto el Defensor del Pueblo como el Grupo Parlamentario Popular, hayan planteado recurso de inconstitucional, ya que, según alegan, sólo podrán establecerse excepciones cuando ponderados los intereses en juego, valorados los peligros potenciales de una y otra opción, deba entenderse que es más grave para el orden constitucional informar al afectado, o permitirle el acceso y rectificación, que negarle el uso de estas facultades.

Las excepciones contenidas en los artículos 2l y 22 hacen referencia, no sólo, a los derechos de acceso, rectificación y cancelación, sino también, a los de información en la recogida de datos y a la privación del consentimiento del afectado.

2) *Ficheros de Titularidad Privada*

Mayor número de artículos dedica la Ley a los ficheros de titularidad privada, del 23 al 3l, ambos inclusive, que son los que constituyen el capítulo II del Título IV. y en ellos se trata: la creación, notificación e inscripción registral, comunicación de la cesión de datos, datos sobre abonados a servicios de telecomunicación, prestación de servicios de tratamiento automatizado de datos de carácter personal, prestación de servicios e información sobre solvencia patrimonial y crédito, ficheros con fines de públicidad, ficheros relativos a encuestas e investigaciones y Códigos tipo.

En los ficheros de titularidad privada, se exige siempre el consentimiento del interesado para recabar los datos, consentimiento, que como hemos apuntado anteriormente, puede ser revocado, pero sin producir efectos retroactivos.

En la cesión de datos, también, es necesario el consentimiento del afectado, que deberá, igualmente, ser informado, por el responsable del fichero, en el momento en que se efectue la primera cesión de datos.

Tienen plena efectividad los derechos de información, acceso, rectificación y cancelación, asi como de cuantas garantías, esta Ley, reconoce a los ciudadanos y que en los ficheros de titularidad privada adquieren plena efectividad, por lo que no es necesario repetir lo que sobre cada uno de ellos hemos apuntado anteriormente.

Toda persona o entidad que proceda a la creación de ficheros automatizados de datos de carácter personal lo notificará "previamente" a la Agencia de Protección de Datos, haciendo constar, además de lo que reglamentariamente se establezca, el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad y las cesiones que se preveean. Tras la notificación a la Agencia, pueden darse dos supuestos: que la Agencia de Protección de Datos resuelva o que deje transcurrir el tiempo sin resolver.

En caso de resolución, ésta, corresponde, en base al artículo l2.2.a), del Real Decreto 428/l.993, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, al Director de la Agencia de Protección de Datos y debera ser motivada sobre la procedencia o improcedencia de la inscripción en el Registro General de Protección de Datos; con su decisión se agota la via administrativa, contra la que cabe recurso contencioso-administrativo, según el artículo l7.1 de la Ley y art. 2.4 del Estatuto de la Agencia de Protección de Datos.

Si no hubiese resolución, transcurrido un mes desde la presentación de la solicitud de inscripción, sin que la Agencia de Datos hubieda resuelto sobre la misma, se entenderá inscrito el fichero aumatizado a todos los efectos (art. 24).

Según la disposición adicional segunda de la Ley los ficheros existentes, en el momento de entrada en vigor de la presente Ley, deberán inscribirse dentro del año siguiente, plazo ampliado por Real Decreto-Ley, 2O/1993, por seis meses más, es decir hasta el 3l de julio de l.994.

Los responsables de ficheros de titularidad privada podrán formular códigos tipo que establezcan las condiciones de organización, funcionamiento, procedimiento, normas de seguridad, programas, obligaciones..., que tendrán el carácter de códigos deontológicos o de buena práctica profesional y que deberán ser depositados o inscritos en el Registro General de Protección de Datos.

En las líneas precedentes hemos apuntado las principales reglas comunes a todo fichero de titularidad privada, que recoge el capítulo II, en el que a su vez aparecen una serie de disposiciones que se refieren a aspectos singulares de los que se ocupan de unas determinadas finalidades, como a solvencia patrimonial, publicidad, encuestas o investigaciones...

G) MOVIMIENTO INTERNACIONAL DE DATOS

El título V de la Ley, bajo el epígrafe de "movimiento internacional de datos" comprende los artículos 32 y 33 y regula la transferencia de datos transfronteras y sus requisitos, de acuerdo con la protección existente en el destino, que debe ser equiparable al que presta la presente Ley (art. 32).

En este punto, como en otros de la ley, hay una terminología distinta en la exposición de motivos, donde se habla de "transmision internacional de datos", "flujo internacional de datos", para utilizar en el artículado la expresion "transferencia" y enunciar el capítulo con el de "movimiento internacional de datos".

Se pone en manos del Director de la Agencia de Protección de Datos el determinar qué entiende por equiparable y por tanto si hay o no garantía, en otros paises, para transmitir los datos de carácter personal.

En los dos artículos, que regulan la materia, no aparece epígrafe alguno destinado a regular la importación de datos personales de otros paises.

El artículo 33 regula, una vez más, una serie de excepciones, tales como: cuando resulte de tratados o convenios; a efectos de prestar o solicitar auxilio judicial internacional; de datos de carácter médico entre facultativos o instituciones sanitarias; o cuando se refiera a transferencias dinerarias.

H) AGENCIA DE PROTECCION DE DATOS

Como Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada ,se regula , en el Titulo VI de la LORTAD, artículos 34 a 4l, el órgano de fiscalización y control bajo el nombre de Agencia de Protección de Datos.

El título VI de la Ley Orgánica 5/l.992, crea la Agencia de Protección de Datos y dispone, en su artículo primero, que se regirá, fundamentalmente, por lo dispuesto en dicha Ley y en un Estatuto propio que será aprobado por el Gobierno y que así lo hizo, por Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

Tiene como misiones primordiales velar por el cumplimiento de la Ley, dictar instrucciones, sancionar las infracciones de caracter administrativo previstas en ella, atender las reclamaciones de los interesados, y redactar la memoria anual.

En la estructura orgánica, de la Agencia de Protección de Datos, destaca la figura del director de la misma que será nombrado por Real Decreto, de entre quienes componen el Consejo Consultivo, por un período de cuatro años.

Al Director, órgano unipersonal, le corresponde la representación de la Agencia de Protección de Datos y, en exclusiva, las facultades ejecutivas y la suprema capacidad de decisión dentro de la Agencia, asistido por un Consejo meramente consultivo. Puede decirse, por ello, que la Agencia es el Director, toda vez que la función asesora del Consejo Consultivo sólo se ejerce a instancia del Director, sin perjuicio de formular propuestas en temas relacionados con las materias de la competencia de la Agencia (art. l8 del Estatuto).

No obstante destacar la exposición de motivos la absoluta independencia del Director, lo cierto es que el mismo es nombrado por el ejecutivo a quien también corresponde su cese, a diferencia de lo que es norma habitual del derecho comparado, que lo nombra el Parlamento, por lo que se ha puesto en duda su absoluta independencia.

El Director permanece en el cargo por un plazo de cuatro años, al igual que los vocales del Consejo Consultivo. Su inamovilidad, durante este período, y el establecimiento, en el artículo 15 del Estatuto, de forma tasada, las causas de cese o separación del Director ha dejado de ser éste uno de los aspectos más controvertidos de la Ley, si bien al ser una de las causas "el incumplimiento grave de las obligaciones del cargo", circunstancia por completo carente de la certeza y concreción necesaria, pone en duda su absoluta independencia.

Según el artículo 2 del Estatuto, los actos del Director se consideran actos de la Agencia y agotan la via administrativa, no están sujetos, por tanto, a modalidad alguna de tutela administrativa. Contra ellos se podrán interponer los recursos contencioso-administrativos que resulten procedentes.

El Consejo Consultivo está integrado por nueve miembros propuestos uno por cada una de las siguientes instituciones: Congreso de los Diputados, Senado, Administración Central, Autonómica, Local, Universidad, usuarios, Academia de la Historia y un representante del sector de ficheros privados.

Junto al Director y Consejo Consultivo, la estrutura de la Agencia se completa, según el art. 11 del Estatuto, con el Registro General de Protección de Datos -donde serán objeto de inscripción, los ficheros automatizados de que sean titulares las Administraciones Públicas, los ficheros privados, las autorizaciones y los códigos tipo (art.30 de la Ley)- la Inspección de Datos y la Secretaría General, como órganos jerárquicamente dependientes del Director de la Agencia.

Acogiéndose al artículo 40 de la LORTAD, que permite la asignación de competencias a las comunidades autónomas, a iniciativa de la Comisión de Libertades e Informática de la Comunidad Valenciana (CLIVA), el Magistrado Jesús Martínez Arenas, ha elaborado una propuesta de Ley Autonómica de Regulación del Tratamiento Automatizado de Datos de Caracter Personal, ya que según el Sr. Martínez Arenas "es necesario extender la Ley al ámbito autonómico porque existen marcos de legislación propios a los que no tiene acceso la Administración Central y donde se produce la utilización de datos de los ciudadanos".

I) INFRACCIONES Y SANCIONES

Al título VII bajo el epígrafe "Infracciones y Sanciones", se dedican los artículos 42 a 48, en los que se trata: responsable, tipo de infracciones, tipo de sanciones, infracciones de las Administraciones Públicas, prescripción, procedimiento sancionador y potestad de inmovilización de ficheros.

Tras establecer el artículo 42 que los responsables de los ficheros estarán sujetos al régimen sancionador establecido en la presente Ley, ésta, tras clasificar las infracciones en leves, graves y muy graves, describe,en el artículo 43, hasta un total de veintiuna infracciones, ampliables a cualquier otra, que se pueda incluir,en las concepciones muy amplias, que a las mismas dan los apartados, 2.d); 3.d) y 4,f) del artículo 43.

Los tipos de infracciones pretenden proteger los derechos de información, acceso, rectificación y cancelación, movimiento internacional de datos, secreto, cesión, calidad de datos, consentimiento, datos especialmente protegidos, creacion de ficheros...

La cuantía, de las sanciones previstas, se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad y a la reincidencia (art. 44.4).

Las sanciones previstas, en el art. 44, son pecuniarias y solo afectan a los titulares de ficheros privados, con multa que va de:

100.000 a 10.000.000 .....para las infracciones leves
10.000.001 a 50.000.000 .....para las infracciones graves
50.000.001 a 100.000.000 .....para las muy graves

El tope mínimo, 100.000 pesetas, nos parece excesivo, al igual que bajo, el tope máximo, por infracciones muy graves, que, por otra parte, queda ponderado al disponer, el art.48, que en los supuestos, constitutivos de infracción muy grave, -de utilización o cesión ilícita de los datos de carácter personal en el que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de su personalidad que la Constitución y las Leyes garantizan- el Director de la Agencia de Protección de Datos, podrá requerir a los responsables del fichero a la cesación en la utilización o cesión ilícita de los datos y si este requerimiento fuese desatendido, podrá, mediante resolución motivada, inmovilizar tales ficheros, tanto públicos como privados, a los solos efectos de restaurar los derechos de las personas afectadas.

El sistema de sanciones de los artículos 43 y 44 sólo afecta a los titulares de ficheros privados, pues como dice Heredero Higueras[12], no tendría carác-

■ 12 HEREDERO HIGUERAS, Manuel: "La Ley Orgánica 5/1992, de 29 de Octubre, de Regulacion Del Tratamiento Automatizado de los Datos de Carácter Personal", Boletín de información del Ministerio de Justicia núm. I669, Madrid I993.

ter disuasorio alguno imponer sanciones pecuniarias a un órgano de una Administración Pública, pues la sanción se resolvería en una adscripción o transferencia a favor del Tesoro, de parte de un crédito del presupuesto del órgano que incumpliera la Ley. Por ello, el artículo 45 prevé un sistema más directo, consistente en ordenar la cesión de un tratamiento de datos que incumpla la Ley y, en su caso, instar actuaciones disciplinarias contra el personal correspondiente.

La potestad sancionadora se encomienda a la Agencia de Protección de Datos, contra cuyas resoluciones, como ya hemos indicado, procederá recurso contencioso-administrativo.

Una vez más, la Ley, en su artículo 47, fija que por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de sanciones a que hace referencia el presente título.

J) DISPOSICIONES ADICIONALES, TRANSITORIA, DEROGATORIA Y FINALES

Termina la Ley con tres disposiciones adicionales, una disposición transitoria, una derogatoria y cuatro disposiciones finales.

Las disposiciones adicionales hacen referencia:

- Al Defensor del Pueblo,

- Exclusiones de la aplicación de los Títulos VI y VII -relativos a la Agencia de Protección de Datos y al régimen de infracciones y sanciones- a los ficheros de los que sean titulares las Cortes Generales, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo General de Poder Judicial y el Tribunal Constitucional. Ello quiere decir, a sensu contrario, que sí les serán de aplicación las normas contenidas en el título II, relativo a los principios de protección de datos, y en el título III, referente a los derechos de las personas.

- El plazo, para que los, aproximadamente 200.000 ficheros existentes, al entrar en vigor la LORTAD, lo comuniquen a la Agencia de Protección de Datos. Según la disposición adicional segunda, tendrá lugar dentro del año siguiente a la entrada en vigor de la presente Ley, plazo que, el Real Decreto Ley 20/1.993, de 22 de diciembre (B.O.E. núm. 3l0,de 22 de diciembre) ha prorrogado por seis meses, es decir hasta el 3l de julio de l.994, el plazo de un año establecido en la citada disposición adicional, para solicitar la inscripción en el Registro General de Protección de Datos.

La disposición transitoria pretende la adaptación de los ficheros automatizados existentes a la normativa introducida por la LORTAD, y para ello establece igualmente el plazo de un año desde la entrada en vigor de la Ley.

La disposición derogatoria se limita a hacerlo de la disposición transitoria primera de la Ley Orgánica 1/82, de 5 de mayo, de protección civil del derecho al honor, a la intimidad pesonal y familiar y a la propia imagen.

Las cuatro disposiciones finales nos ponen de manifiesto:

- El mandato dado al Gobierno para dictar las disposiciones necesarias para el desarrollo de esta Ley.

- La extensión, si lo considera oportuno, de la aplicación de la Ley a ficheros convencionales, por parte del Gobierno, previo informe del Director de la Agencia de Protección de Datos.

- Los preceptos, artículos 18, 19, 23, 26, 27, 28, 29, 30, 31, los Títulos VI y VII, las disposiciones adicionales primera y segunda y la disposición final primera, que tienen carácter de Ley ordinaria.

- El momento de entrada en vigor de la Ley, a los tres meses de su publicación en el Boletín Oficial del Estado, por lo que, si tenemos en cuenta que, la Ley fue publicada en el BOE del día 31 de octubre de 1.992, su entrada en vigor tuvo lugar el día 31 de enero de 1.993.

Con esto damos por finalizado el rápido recorrido efectuado por la Ley y de la que hemos ido tocando los puntos fundamentales de la misma, por considerarlo importante, pues se ha señalado por parte de la doctrina española y extranjera que este nuevo derecho corresponde, junto con los de, por ejemplo, los consumidores o el de la calidad de vida, a una nueva generación de derechos humanos que aparece como respuesta a situaciones que han ido surgiendo en las sociedades más desarrolladas o tecnológicamente avanzadas.

VII.- Las Autopistas de la Información

Si lo apuntado, anteriormente, nos denota la conveniencia de la LORTAD, en las decadas pasadas, todavía lo es más en la que nos encontramos en la que las "autopistas de la información" son consideradas como el gran reto tecnológico de los próximos años. Mediante la interrelación del ordenador, la televisión y el teléfono, con potentes líneas de fibra óptica o vía satélite, se

podrán transportar millones de datos, imágenes y sonido, simultaneamente, a gran velocidad y calidad, toda vez que las redes de banda ancha, transmiten datos, imágenes, textos y voz de forma integrada a velocidades del orden de los 600 millones de elementos (bits) por segundo. Esta velocidad es unas 10.000 veces superior a las denominadas redes de banda estrecha.

La banda ancha reune tres características esenciales: rapidez, fiabilidad y flexibilidad, lo que hace sea apta para la necesidad de transmisión de datos personales que serán comunicados a muy alta velocidad y permitirán conectar las redes informáticas con otras del exterior, facilitando además el uso del terminal multimedia.

En Estados Unidos, la industria privada considera que las posibilidades de las "superautopistas" de las comunicaciones son casi infinitas, aunque todavía es prematura vaticinar hasta donde podrán llegar los servicios que prestará la nueva tecnología.

El tema de las "autopistas de la información" es tan importante que diecinueve expertos integran el panel recientemente constituido por la Comisión Europea, para encontrar soluciones técnicas y administrativas que permitan la creación, en Europa, de una "superautopista" de información, similar a la que impulsa en Estados Unidos el vicepresidente Albert Gore.

El monopolio de las operadoras impiden en Europa las "autopistas" de la información, toda vez que Europa dispone de las tecnologías necesarias para hacer frente a este reto. No obstante, el gran problema consiste en las actuales barreras normativas que impiden el desarrollo de estas redes supranacionales, que deberían ir acompañadas de una Directiva Comunitaria que tenga en cuenta la incidencia de estas "superautopistas de la información" en los datos de carácter personal, al igual que los paises miembros aprueben disposiciones que mejoren la protección de los datos personales, teniendo en cuenta la incidencia que sobre ellos puede tener la evolución tecnológica que nos llevará a las "autopistas de la información" y a la insuficiencia de la LORTAD.

VIII.- Bibliografía

Queremos concluir, este trabajo, recogiendo, no sólo, la bibliografía utilizada en el mismo sino una bibliografía más amplia, de libros o artículos públicados, en lengua española, sobre el tema.

ALBACAR LOPEZ, José Luis; "La protección de los derechos fundamen-

tales en la nueva Constitución Española", Ministerio del Interior, Madrid, 1979.

ALENDE, Jorge Oscar: "Informática: el abuso de su poder", En: Informática y Derecho, nº.4, UNED-Merida, 1993.

ALVAREZ CIENFUEGOS SUAREZ, José María: "El derecho a la intimidad personal, la libre difusión de la información y el control del estado sobre los bancos de datos", En: Actualidad Administrativa, (nº 37), 1991.

ALONSO BALLESTEROS, Mª del Pilar: "La incidencia en la empresa de la Ley Orgánica 5/1.992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal", Actualidad financiera, núm. 47, 1992.

ALONSO ROYANO, Felix: "¿Estado de Derecho o derecho del Estado? (el delito informático)" En: Revista General de Derecho, nº 498, (1986).

AMAT NOGUERA, N: "Documentación científica y nuevas tecnologías de la información", Pirámide, 1987.

ARROYO YANES, Luis Miguel: "La cancelación de datos personales en ficheros de titularidad pública en el proyecto de LORTAD en España", En: Informática y Derecho nº. 4, UNED-Mérida, 1993.

ASPAS ASPAS, José Mª: "El Derecho a la autodeterminación informativa en la Ley Portuguesa de Protección de Datos de 1991. Sujetos, contenidos y garantías" En: Informática y Derecho nº.4, UNED-Mérida, 1993.

BERMEJO VERA, José: "Premisas jurídicas de la intimidad personal y de la protección de los datos en el derecho español" Libro homenaje al profesor José Luis Villar Palasi, Civitas, Madrid, 1989, p. 143-162.

BIANCHINI, R. y OTROS: "Seguridad en la electrónica e informática" Mapfre, 1983.

BLAS ZULUETA, Luis: "Delitos informáticos", En: Revista General de Derecho, n. 495, 1985.

BLAZQUEZ ANDRES, Mª Consuelo y OTROS: "Intimidad personal y limitaciones". En: Informática y Derecho nº.4, UNED-Mérida 1993.

BOIX REIG, J.: "Protección juridico-penal de la intimidad e informática", En: revista Poder Judicial, núm 9-especial, 1988.

BOIX REIG, J.: "Consideraciones sobre la protección penal de la intimidad y del honor e informática", En: Informática e Diritto, nº 2, 1989.

BUQUICCHIO, Giovanni: "Informática y Libertades: balance de quince años de actividad del Consejo de Europa" En: Jornadas Internacionales sobre Informática y Administración Pública, Instituto Vasco de Administración Pública, 1986.

BUTTARELLI, Giovanni: "Banche dati e tutela della personalità", Documenti giustizia, núm.1O/ octubre, 1992.

CAMACHO LOSA, L.: "El delito informático", Camacho Losa, 1987.

CAMPANELLA DE RIZZI, Elena: "Informática y derecho a la intimidad", Actas de primer Congreso Iberoamericano de Informática y Derecho, CREI, 1985.

CARRASCOSA GONZALEZ, Javier: "Régimen juridico del flujo internacional de datos informatizados de carácter personal", Revista General de Derecho, núm. 577-578, 1991.

CARRASCOSA LOPEZ, V.: "La correcta garantía del derecho a la intimidad", Generalitat de Catalunya, 1993.

CARRASCOSA LOPEZ, V. y OTROS: "La protección de los datos personales. Regulación nacional e internacional de la seguridad informática", Centre d'Investigació de la Comunicació i Universitat Pompeu Fabra, Generalitat de Catalunya, 1993

CARRASCOSA LOPEZ, V.: "El ordenador un instrumento eficaz del delito", En: Revista Proserpina, núm. 5, Universidad a Distancia, Mérida, 1992.

CARRASCOSA LOPEZ, V y OTROS: "El derecho de la prueba y la informatica", En: Informática y Derecho núm. 2, UNED-Mérida, 1991.

CARRASCOSA LOPEZ, V.: "Control de Sistemas Informáticos en la oficina judicial española", Asociación de Abogados de Buenos Aires y la association pour le Developpement de l´ Informatique Juridique, 1990.

CARRASCOSA LOPEZ, V.: "Informática en la Oficina Judicial, Materias para una reforma procesal", Ministerio de Justicia, Madrid, 1991.

CARRASCOSA LOPEZ, V.: "Nuevas tecnologías en la oficina judicial" Revista de Derecho Procesal, Madrid, 1988.

CARRASCOSA LOPEZ, V.: "El impacto de las tecnologías de la información y las telecomunicaciones en el auxilio judicial", CREI, 1993.

CARRASCOSA LOPEZ, V,: "El derecho informático en España", Revista ICADE, Madrid, 1989.

CARRASCOSA LOPEZ, V.: "Informática jurídica e gestao judicial", Boletin Da Orden dos Advogados, núm. 14, Lisboa, MIO/1983.

CARRASCOSA LOPEZ, V.: "Bases de datos jurisprudenciales y legales", Actas Congreso Internacional de Informática y Derecho, ADIJ, Buenos Aires, 1990.

CARRASCOSA LOPEZ, V.: "La automatización del Registro Civil: Las tecnologías de la información y las comunicaciones al servicio del ciudadano", MAP, Valencia, 1991.

CARRASCOSA LOPEZ, V.: "Administración de justicia y nuevas tecnologías", Encuentros sobre Informática y Derecho 1990-1991, ICADE - ARANZADI, 1992.

CARRASCOSA LOPEZ, V.: "Derecho a la intimidad e informática", Escuela Universitaria Politécnica, Mérida, 1983.

CARRASCOSA LOPEZ V. y OTROS: "La protección de datos personales en la Península Ibérica", En: Informatica y Derecho", núm. 4, UNED-Mérida, 1993.

CARRASCOSA LOPEZ, V.: "Nuevas tecnologías de la Información y las comunicaciones en la Secretaría Judicial", VI Jornadas de Fe Pública Judicial, Colegio Nacional de Secretarios Judiciales, Granada 1993.

CARRASCOSA LOPEZ, V. y OTROS: "Intimidad personal y limitaciones", En: Informática y Derecho, nº 4 - UNED- Mérida, 1993.

CARRASCOSA LOPEZ, V.: "Derecho a la intimidad e informática", En: Informática y Derecho, nº.1, UNED-Mérida, 1992.

CASTELLS ARTECHE, José Manuel: "La limitación informática", En: Estudios sobre la Constitución Española: homenaje al profesor Eduardo Garcia de Enterría, Madrid, Cívitas, 1991.

CASTELLS ARTECHE, José Manuel: "Otra asignatura pendiente: El control de la informática", En: Jueces para la Democracia, 1989.

CASTILLO JIMENEZ, Mª. Cinta: "Análisis comparativo entre la Ley 10/91 portuguesa y el proyecto de LORTAD de nuestro país", En: Informática y Derecho, nº 4, UNED-Mérida, 1993.

CORREA, CARLOS M. Y OTROS: "Derecho Informático". De Palma, Buenos Aires. 1987.

DAVARA RODRIGUEZ, M. A.: "La ley española de protección de datos: ¿una limitación del uso de la informática para garantizar la intimidad?", En: Actualidad Jurídica Aranzadi, l2 y l9 de noviembre de 1992.

DAVARA RODRIGUEZ, M.A.: "La protección de las personas en lo referente al tratamiento automatizado de sus datos personales", Anuario Jurídico Escurialense, núm 23, 1991.

DAVARA RODRIGUEZ, M.A.: "Derecho Informático", Aranzadi, 1993.

DE CARTOLANO, Silvia C.: "Reforma de la constitución de Rio Negro: necesidad de introducir el tema "informática y protección de datos personales"", En: Informática y Derecho, nº 4, UNED-Mérida, 1993.

DE JULIOS CAMPUZANO, Alfonso: "Derecho a la intimidad y publicidad de los datos personales de carácter patrimonial" En: Informática y Derecho, nº 4, UNED-Merida 1993.

DE VAL ARNAL, José Luis: "La presunción de inocencia y el deber de colaboración con la inspección de trabajo: Derecho de acceso a los archivos informáticos". En: Informática y Derecho, nº 4, UNED-Mérida, 1993.

DRESNER, Stewart H.: "Spain adapts to a new european privacy future", Generalitat de Catalunya, 1993.

ESTRADA ALONSO, E.: "El derecho al honor en la Ley Orgánica l/1.982, Civitas, 1988.

FARIÑAS MATONI L.M.: "El derecho a la intimidad", Trivium, 1983.

FARRIOLS SOLA, Antonio: "La Agencia de protección de datos: una consecuencia de la Ley Orgánica 5/1.992", En: actualidad informática Aranzadi, nº 9, 1993.

FERNANDEZ PABLO, Rafael: "Datos personales: tecnología, ley y ética", En: Actualidad informática Aranzadi, nº 8, Madrid, 1993.

FERNANDO PABLO, Marcos Matías: "Administración Pública, Informática y ciudadano: perspectiva general", En: Informática y Derecho, nº 4, UNED-Mérida, 1993.

FRIGINAL FERNANDEZ- VILLAVERDE, Luis: "La protección de los derechos fundamentales en el ordenamiento español", Madrid, Montecorvo, 1981.

FROSINI, V.: "Bancos de datos y tutela de la persona", Revista de Estudios Políticos, n.30, 1982.

FROSINI, V.: "Cibernética, Derecho y Sociedad", Tecnos, 1982.

FROSINI, V.: "La convenzione europea sulla protezione dei dati", Revista di Diritto Europeo, núm. I-III, 1984.

FROSINI, V.: " Informática y derecho", Temis, Bogotá, 1988.

FROSINI, V.: "Los derechos humanos en la sociedad tecnológica", Anuario de derechos humanos, 1982-1983.

GAYO SANTA CECILIA, Mª Eugenia: "Garantías del ciudadano ante la LORTAD: posibles vías de defensa y protección de sus derechos fundamentales", En: Informática y Derecho, nº 4, UNED-Mérida, 1993.

GEBHARDT, H. P.: "Principios jurídicos de la protección de datos y de la protección de datos en el sector de las telecomunicaciones en siete paises: Suiza, Francia, República Federal de Alemania, Reino Unido, Suecia, Estados Unidos y Japón", En: Boletín de Telecomunicaciones, 1990.

GOMEZ DEL POZUELO, E.: "Las empresas de marketing directo. La Ley orgánica de regulación del tratamiento automatizado de datos y su aplicación." Generalitat de Catalunya, 1993.

GONZALEZ PEREZ, Jesús: "La dignidad de la persona", Madrid, Civitas, 1986.

GONZALEZ RIVAS J.J. y OTROS: "Doctrina del Tribunal Constitucional, Tribunal Supremo, Tribunal Central de Trabajo y Tribunal Europeo de Derechos Humanos", Colex, 1988.

GONZALEZ RUS J.J.: "Aproximación al tratamiento penal de los ilicitos patrimoniales relacionados con los medios o procedimientos informáticos", Revista de la Facultad de Derecho de la Universidad Complutense de Madrid, núm.12, 1986.

GONZALEZ RUIZ, Francisco Javier: "La protección de derechos fundamentales frente al tratamiento automatizado de datos personales", Revista de estudios e investigación de las Comunidades Europeas, nº 21, 1991.

GUASTAVINO, E.P.: "Responsabilidad civil y otros problemas jurídicos en computación", La Roca, Buenos Aires, 1987.

HEREDERO HIGUERAS, M.: "Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal", Boletín de Información del Ministerio de Justicia, núm 1669, Madrid 1993.

HEREDERO HIGUERAS,M." "Legislación informática"., Tecnos, 1994.

HEREDERO HIGUERAS,M.: "La protección de datos personales en manos de la policía: reflexiones sobre el Convenio de Schengen", Generalitat de Catalunya, 1993.

HEREDERO HIGUERAS, M.: "La protección de los datos de carácter personal registrados en soporte informatizado con fines estadisticos, en el Derecho español, En: informática y derecho, núm 4, UNED-MERIDA, 1993.

HEREDERO HIGUERAS, M.: "El Convenio del Consejo de Europa sobre protección de datos", Documentación Administrativa núm. 199, 1983.

HEREDERO HIGUERAS, Manuel: "La protección de los datos personales registrados en soportes informáticos, En: Actualidad Informática Aranzadi, núm.2, 1992.

HERRERO TEJEDOR: "Honor, Intimidad y propia imagen" Colex, 1990.

HIXSON, Richard F.: "Privacy in a public society", Oxford University Press, Nueva York / Londrés, 1987.

JOINET, Louis: "Orientaciones principales de la Ley francesa relativa a la informática, ficheros y las libertades", En: Documentación Administrativa nº.178, 1978.

LARA GUITARD, Alfredo: "Derecho a la información frente al derecho a la intimidad", Revista española de documentación científica, 1984.

LOPEZ BUSTOS y OTROS: "Uso de la informática por la administración y posible violación del derecho a la intimidad", Revista de la Facultad de Derecho de la Universidad de Granada, 1984.

LOPEZ GARRIDO, Diego: "El proyecto de Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter personal: la excepcionalidad como norma", En: Jueces para la Democracia, nº 13, 1991.

LOPEZ GUERRA, Luis: "La libertad de información y el derecho al honor" En: Jornadas de Protección Jurisdiccional de los Derechos Fundamentales y Libertades Públicas, Cáceres, 1989.

LOPEZ-IBOR MAYOR, Vicente: "Los límites al derecho fundamental a la autodeterminación informativa en la Ley Española de Protección de Datos", En: Actualidad informática Aranzadi, nº.8, Madrid, 1993.

LOPEZ JACOISTE, José Javier: "Intimidad, honor e imagen ante la responsabilidad civil", En: homenaje a Juan Berchmans Vallet de Goytisolo, Consejo General de Notarios, 1988.

LOSANO, M.: "Curso de Informática Jurídica", Tecnos, 1987.

LOSANO, M. y OTROS: "Libertad informática y leyes de protección de datos personales", Centro de Estudios Constitucionales, Madrid, 1989.

LOSANO, M.: "Los proyectos de Ley italianos sobre la protección de los datos personales", Madrid, Tecnos, 1987.

LUCAS MURILLO DE LA CUEVA, P.: "El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática", Madrid, Tecnos, 1990.

LUCAS MURILLO DE LA CUEVA, P.: "Informática y protección de Datos Personales", Centro de Estudios Constitucionales", Madrid, 1993.

LUCAS MURILLO DE LA CUEVA, P.: "La proteccion de datos personales ante el uso de la informática", En: Revista de la Facultad de Derecho de la Universidad Complutense, nº. l5, 1989.

MADEC, A.: "El mercado internacional de la información. "Los flujos transfronteras de información y datos"", Fundesco/Tecnos, 1984.

MADRID CONESA, F.: "Derecho a la intimidad, informática y estado de derecho, Universidad de Valencia, 1984.

MANNA, Adelmo: "La tutela penal de los derechos de la personalidad: aspectos problemáticos, Cuadernos de Política Criminal, nº 34, 1988.

MARTIN BERNAL, José Manuel y OTROS: "Intimidad y libertades", En: Informática y Derecho, nº.4, UNED-Merida, 1993.

MARTINE FABRE: "Metodología para la Creación de Bancos de Datos Personalizados", En: Informática y Derecho, nº.l, UNED-Mérida, 1992.

MARTIN ONCINA, José Ignacio: "La protección de datos informáticos en el derecho comparado", En: Informática y Derecho, nº. 4, UNED-Mérida 1993.

MARTIN PALLIN, Jose Antonio y OTROS: "La informática: un riesgo incontrolado. Propuesta para texto articulado sobre la Ley para la Protección de derechos y libertades en relación con el uso de la informática y las telecomunicaciones", En: Revista Vasca de Administración Pública, nº.20, 1988.

MARTINEZ ECHEVERRIA, Miguel A.: "Informática y derechos humanos". En: Persona y Derecho, nº 15, 1988.

MASUDA, Y.: "La sociedad informatizada como sociedad postindustrial", Fundesco/Tecnos, 1984.

MEJIA GOMEZ, Beatríz Elena: "La informática jurídica. Atenta contra la libertad individual", Actas I Congreso Iberoamericano de Informática y Derecho, CREI, Madrid, 1985.

MIGUEL CASTAÑO, A de: "Derecho a la información frente al derecho a la intimidad. Su incidencia en el servicio de información estadística", Madrid, 1983.

MIGUEL CASTAÑO, A de: "Derecho a la intimidad frente al derecho a la información. El ordenador y las leyes de protección de datos", Revista General de Legislación y Jurisprudencia, n 4, 1983.

MIGUEL CASTAÑO, A de: "Libertad de información y derecho a la intimidad: medios para garantizarlos. Incidencia en el ambito de la estadística", Revista de la Facultad de Derecho de la Universidad Complutense de Madrid, núm, 12, monográfico, 1986.

MONTERO, ETTIENNe: "Las obligaciones y responsabilidades del "titular" de un fichero de datos nominativos en cuanto a la cualidad de su producto", En: Iinformática y Derecho, n°.4, UNED-Mérida, 1993.

MORALES PRATS,F.: "La tutela penal de la intimidad: privacy e informática", Ediciones Destino, Barcelona, 1984.

MURRAY LAVER: "Los ordenadores y el cambio social", Fundesco, 1982.

NARVAIZA SOLIS, José Luis: "Etica y estadística: el tratamiento de los datos en la legislación española", En: Boletín de Estudios Económicos, n° l44, 1991.

NASARRE GOICOECHEA, E.: "El artículo l8.4 de la Constitución visto desde el Defensor del Pueblo", Fundación Citema.- 1985.

NIBLETT, B.: "Data Protection Act", London, Longman 1.984, 1984.

NORA, S y MINC, A.: "La informatización de la sociedad", Fondo de Cultura Económica, 1980.

OLIVEROS LAPUERTA, María Vicenta: "Estudios sobre la ley de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, Madrid 1980.

OROZCO PARDO, Guillermo: "Consideraciones sobre los derechos de acceso y rectificación en el proyecto de Ley Orgánica de regulación del trata-

miento automatizado de los datos de carácter personal", En: Informática y Derecho, nº 4, UNED-Mérida, 1993.

ORZABAL, Josefina C.: "Bases de datos, privacidad y responsabilidad civil", En: Informática y Derecho, nº 4, UNED-Mérida, 1993.

PAEZ MAÑA, Jorge: "La incidencia de la LORTAD en los procesos de producción y distribución de ficheros", En: Actualidad informática Aranzadi, nº.7, Madrid, 1993.

PEDROL RIUS, A: "Escuchas telefónicas", Boletín del Colegio de Abogados de Madrid, nº 1, 1991.

PEREZ LUÑO, A. E.: "Nuevas tecnologías, sociedad y derecho. El impacto de las N.T. de la información", Fundesco, Madrid, 1987.

PEREZ LUÑO, A. E.: "La protección de datos personales en España: presente y futuro", En: Informática y Derecho, nº 4, UNED, Mérida, 1993.

PEREZ LUÑO, A. E.: "Informática y libertad, comentario al artículo l8.4 de la Constitución", Revista de Estudios Políticos, 198l.

PEREZ LUÑO, A. E.: "La protección de la intimidad frente a la informática en la Constitución española de 1.978", Revista de Estudios Políticos, 1979.

PEREZ LUÑO, A. E.: "La protección de los datos personales en España", Estudios jurídicos en honor de José Gabaldón López, Trivium, 199O.

PEREZ LUÑO, A. E.:"La contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo", En Anuario de Derechos Humanos, tomo 4, 1987.

PEREZ LUÑO, A. E.: "Derechos humanos, Estado de Derecho y Constitución", Tecnos, 4º ed, Madrid, 1991.

PEREZ LUÑO, A. E.: "Nuevos derechos fundamentales de la era tecnológica: la libertad informática", En: Anuario de Derecho Público y Estudios Políticos, n.2, 1989-1990.

PEREZ LUÑO, A.E.: "La defensa del ciudadano y la protección de datos", En: Revista Vasca de Administración Pública, n.14, 1986.

PEREZ LUÑO, A. E.: "Del habeas corpus al habeas data", En: Informática y Derecho, nº. l, UNED-Mérida, 1992.

PIÑOLL i RULL, J.: "Los flujos internacionales de datos: aproximación a su regulación jurídica", UNED, T. IV, Barbastro, 1987.

PIÑOL i RULL, J. L y OTROS.: "La regulación del flujo internacional de datos, Generalitad de Catalunya, 1993.

POMED SANCHEZ, Luis Alberto: "El Derecho de acceso de los ciudadanos a los archivos y registros administrativos", Instituto Nacional de Administración Pública, Madrid, 1989

PRADA ALVAREZ-BUYLLA, Plácido.: "La publicidad registral y el derecho a la intimidad, Revista crítica de derecho inmobiliario, 1992, 610.

PUENTE MUÑOZ, Teresa: "El derecho a la intimidad en el artículo l8 de la Constitución", En: Estudios sobre la Constitución Española de 1.978, Universidad de Valencia, Valencia, 1980.

QUILEZ AGREDA, Ernesto: "Sobre la inconstitucionalidad de la Ley de Protección de Datos", En: Actualidad informática Aranzadi, nº.9, Madrid, 1993.

RAMIRO LOZANO, Inmaculada y OTROS: "La protección de datos personales en la Península Ibérica", En: Informática y Derecho, nº.4, UNED, Mérida 1993.

REY GUANTER, Salvador del: "Relación laboral y tratamiento automatizado de datos de carácter personal", núm. 4, Revista Xurídica Galega, 1993.

RIPOL CARULLA, Santiago: "Valoración española del proyecto de directiva comunitaria sobre protección de datos (contribución al estudio de la noción de posición nacional)", En: Informática y Derecho, nº. 4, UNED-Mérida, 1993.

RIPOLLES SERRANO, María Rosa y OTROS: "Derecho al honor e intimidad y derecho de información", En: Revista de las Cortes Generales, n. l6, 1989.

ROCA ROVIRA, J.C.: "Normas básicas de deontología informática", Citema, 1974.

ROMAN GARCIA, Antonio: "Aportación al estudio de la responsabilidad civil por los daños ocasionados en los bienes y derechos de la personalidad (problemática suscitada por la aplicación de la Ley Orgánica 1/1.982, de 5 de mayo, sobre protección civil del derecho al menor, a la intimidad personal y familiar y propia imagen", Revista de Derecho Privado, 1989, 73 (4).

ROMEO CASABONA, Carlos María: "Poder informático y seguridad jurídica", Fundesco, 1987.

ROMEO CASABONA, Carlos María: "Las nuevas tecnologías de la información: un nuevo desafio para el derecho, Telos, 1988.

ROMEO CASABONA, Carlos María: "Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías", En: Poder Judicial, nº 31, 1993.

ROMERO COLOMA, A. M.: "Derecho a la intimidad, a la información y proceso penal", Madrid, Colex, 1987.

SAENZ GIL, Rubén: "Protección de las personas respecto al tratamiento automatizado de datos personales. Normativa Europea. Proyecto de Ley española.- En: Informática y Derecho, nº.4, UNED-Mérida, 1993.

SANCHEZ BRAVO, Alvaro Avelino: "El tratamiento automatizado de las Bases de Datos en el marco de la Comunidad Económica Europea: su protección", En: Informática y Derecho, nº.4, UNED-Mérida, 1993.

SANCHEZ DE DIEGO FERNANDEZ DE LA RIVA, Manuel: "La transparencia de las bases de datos como mecanismo de protección de la intimidad de las personas", En: Informática y Derecho, nº. 4, UNED-Mérida, 1993.

SANCHEZ JIMENEZ, Enrique: "Los derechos humanos de la 3ª generación: la libertad informática", En: Informática y Derecho, nº.4, UNED-Mérida, 1993.

SANTAMARIA IBEAS, José Javier: "La LORTAD: breve análisis de sus antecedentes", En: Informática y Derecho, nº 4, UNED-Mérida, 1993.

SANZ CAJA, V.: "Vulnerabilidad y seguridad de los sistemas informáticos", Fundación Citema, 1982.

SEMPERE RODRIGUEZ, César: "Derecho al honor, a la intimidad y a la propia imagen (art. 18 de la C. E.)" En: Comentarios a las leyes políticas: constitución española de 1.978, Dirigido por Oscar Alzaga Villaamil, Madrid, Edersa, 1984.

SERRANO ALBERCA , José Manuel: "Derecho al honor, a la intimidad personal y familiar y a la propia imagen (art. l8 de la C.E.)", En: Comentarios a la Constitución, Dirigido por Fernando Garrido Falla, Madrid, Civitas, 1985.

TALBOT, J. R.: "La dirección y la seguridad del ordenador", Editorial Hispano Europea", 1984.

TASENDE CALVO, J. J.: "Notas al Proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal", Poder Judicial, núm. 23, 199l.

TELLEZ VALDES, J: "Derecho informático", Universidad Nacional Autónoma de México, México, 1987.

TERRADO, Federico: "La agencia de protección de datos: regulación orgánica y estatutaria", En: Actualidad Informática Aranzadi, nº9, 1993.

THOMAS A. J. y DOUGLAS, I.J.: "Auditoria Informática", Paraninfo, 1987.

TIRADO ROBLES, Mª. Carmen: "La Comunidad Europea ante la Circulación de Datos Personales. Su protección jurídica"

TONIATTI, Roberto: "Libertad informática y derecho a la protección de los datos personales: princios de legislación comparada", Revista Vasca de Administración Pública, núm. 29, 1991.

TRAVERSI, A: "Il Diritto dell'informatica", Ipsoa, 1985.

ULRICH SIEBER: "La delinquance Informatique", Bruselas, 1990.

URABAYEN, Miguel: "Vida privada e información: Un conflicto permanente", Pamplona, Ediciones Universidad de Navarra, 1977

UWE KALBHEN, y OTROS: "Las repercusiones sociales de la tecnología informática", Fundesco-Tecnos, 1983.

VAN DORSSELLAERE, B.: "Guide Juridique de l'informátique", Dunod Informátique", 1.990.

VELAZQUEZ BAUTISTA, R.: "Protección jurídica de datos personales automatizados", Colex, 1993.

VIDAL MARTINEZ, Jaime: "El derecho a la intimidad en la Ley Orgánica 5-5-1981", Madrid, Montecorvo, 1984.

La LORTAD:
Entre las luces y las sombras

ANTONIO-ENRIQUE PEREZ LUÑO
Catedrático de la Facultad de Derecho
de la Universidad de Sevilla.

Con la promulgación el pasado 29 de Octubre de la Ley Orgánica para la Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) España se incorpora al grupo de Estados que cuentan con normas específicas para la protección de informaciones personales. Se concluye así una larga etapa de incertidumbres y vacíos normativos, al tiempo que se inicia una cargada de expectativas sobre las anheladas virtualidades de la LORTAD para poner coto, y evitar en adelante, los abusos informáticos contra la intimidad perpetrados en nuestro país. Conviene indicar que dicha Ley Orgánica llega tarde y mal. Lo primero, porque desde la promulgación de la Constitución, en virtud del expreso mandato de su art. 18.4, así como de la obligación adquirida por la ratificación en 1984 del Convenio de protección de datos personales del Consejo de Europa, el legislador español debía establecer una norma de tutela de las libertades en relación con el uso de la informática. Este compromiso nacional e internacional se ha visto demorado hasta el presente. Lo segundo, porque cabía el consuelo de confiar que nuestro retraso legislativo nos permitiría beneficiarnos de las experiencias previas del Derecho comparado de la informática. No ha sido así y el texto ahora promulgado presenta algunas deficiencias que pudieron y debieron ser evitadas.

La LORTAD presenta en su **haber**, como uno de sus logros más significativos, la definición de los **principios básicos** que informarán la actuación de los bancos de datos automatizados que procesen informaciones personales (artículos 4 a 11). Entre los mismos figuran los de la calidad de los datos (deberán ser adecuados y pertinentes a los fines para los que se han obtenido, exactos, actualizados...); la *transparencia* (que obliga a informar a los afectados por la recogida de datos personales sobre la finalidad, obligatoriedad, consecuencias y derechos que implica su tratamiento automatizado), el *consentimiento* (como garantía de los afectados que es requisito general para cualquier proceso informatizado de datos personales), la tutela reforzada de los *datos sensibles* (informaciones que hacen referencia a convicciones personales o datos susceptibles de engendrar tratos discriminatorios por motivos de raza, salud, vida sexual...), la *seguridad* (frente a la alteración, pérdida o acceso indebido a los datos personales), el *secreto* (que obliga a no revelar las informaciones personales a quienes intervienen en cualquier fase de su tratamiento automatizado) y la *cesión* (limitada al uso para fines legítimos y con el previo consentimiento del afectado).

El otro aspecto abiertamente positivo de la LORTAD consiste en el reconocimiento y tutela jurídica de la **libertad informática** (a ello se consagran sus artículos 12 a 17). La libertad informática se concibe como el nuevo derecho de autotutela de la propia identidad informática. Su función se cifra en garantizar a los ciudadanos unas facultades de información, acceso y control de los datos que les conciernen. Dicha libertad informática ha sido concebida por la doctrina y la jurisprudencia germanas como un derecho a la autodeterminación informativa, que se refiere a la libertad para determinar quién, qué y con qué ocasión pueden conocer informaciones que conciernen a cada sujeto. En la situación tecnológica propia de la sociedad contemporánea todos los ciudadanos, desde su nacimiento, se hallan expuestos a violaciones de su intimidad perpetradas por determinados abusos de la informática y la telemática. La injerencia del ordenador en las diversas esferas y en el tejido de relaciones que conforman la vida cotidiana se hace cada vez más extendida, más difusa, más implacable. Por ello, al tradicional *habeas corpus* corresponde en las sociedades tecnológicas del presente el *habeas data*. El *habeas data* constituye, en suma, un cauce o acción procesal para salvaguardar la libertad informática, que cumple una función paralela, en el seno de los derechos humanos de la tercera generación, a la que en los de la primera generación correspondió al *habeas corpus* respecto a la libertad física o de movimientos de la persona. No es difícil, en efecto, establecer un marcado paralelismo entre la "facultad de acceso" en que se traduce el *habeas data* y la acción exhibitoria del *habeas corpus*.

Pero junto a estos avances innegables, hay que apuntar en el **debe** de la LORTAD determinados fallos e insuficiencias que no pueden ser soslayados. Así, por ejemplo, sobre la **Agencia de Protección de Datos**, ente de Derecho Público sobre el que gravita la implementación de la LORTAD y de sus garantías, hay que decir de inmediato que constituye uno de los aspectos más negativos e insatisfactorios de la nueva norma. Suscita perplejidad y estupor que la Exposición de Motivos destaque la "absoluta independencia" de su Director. A diferencia de lo que es norma habitual en el Derecho Comparado de los *Ombusdsmen* especializados en la protección de datos, el Director no es nombrado por el Parlamento, sino por el Gobierno a quien también corresponde su cese (art. 35). Además, a diferencia de los *Ombudsmen* para la protección de datos extranjeros que presentan informes anuales (muy importantes para conocer el "quién es quién" en materias de agresiones a las libertades informáticas) a las Cámaras representativas, el Director español lo deberá hacer ante Ministerio de Justicia (art. 36, K). Ello condiciona gravemente el riesgo de convertirse en un mero delegado gubernativo para la informática.

Pero quizás el aspecto más discutible e inquietante de la LORTAD sea el de sus constantes y significativas **excepciones** que limitan el alcance práctico del ejercicio de las libertades informáticas. Los constitucionalistas y, en especial, los estudiosos de los derechos fundamentales, suelen criticar la práctica desvirtuadora de algunos textos normativos que, tras solemnes y generosos reconocimientos de las libertades, recortan su ejercicio y las vacían de contenido al establecer un régimen de excepciones y limitaciones no menos generoso. Por ello, no puede dejar de suscitar inquietud el que la LORTAD, tras proclamar las garantías en orden a la protección de datos y derechos de las personas, establezca excepciones relevantes referidas a: la información de los afectados (art. 5.3); a su consentimiento (art. 6.1); a las garantías de los datos sensibles (art. 7.3); a la posibilidad de que las Fuerzas de Seguridad del Estado puedan informatizar datos sensibles sin control judicial, fiscal o de la propia Agencia de Protección de Datos (art. 20.3); así como a la restricción del derecho a la información y acceso de los ciudadanos a los datos que les conciernen (*habeas data*) elaborados por las Administraciones Públicas por motivos tan vagos como "las funciones de control y verificación" de las mismas y a la supeditación general de la tutela a cuanto afecte a la Defensa Nacional, Seguridad pública, persecución de infracciones penales o administrativas, interés público o intereses de terceros más dignos de protección (art. 22)... Excepciones que pueden afectar al contenido esencial de la garantía reconocida en el art. 18.4 de la Constitución y sobre las que, por tanto, se cierne la sombra de la **inconstitucionalidad**.

En las actuales sociedades avanzadas la protección de datos personales tiende, en definitiva, a garantizar **el equilibrio de poderes y situaciones** que

es condición indispensable para el correcto funcionamiento de una comunidad democrática de ciudadanos libres e iguales. Para su logro se precisa un adecuado ordenamiento jurídico de la informática, capaz de armonizar las exigencias de información propias de un Estado avanzado con las garantías de los ciudadanos. Pero estas normas de Derecho informático exigen, para su plena eficacia, impulsar la conciencia y el compromiso cívicos de hacerlas una experiencia tangible en la vida cotidiana. Es tarea de todos contribuir a evitar una paradoja dramática: compensar nuestro retraso en la incorporación al desarrollo tecnológico con la vanguardia mundial en la piratería del *software*, la delincuencia informática, y las agresiones informáticas a la libertad.

Letra y Espíritu de la LORTAD: ¿Un problema de coherencia?

ALFONSO DE JULIOS CAMPUZANO

Profesor-ayudante del departamento de Filosofía del Derecho de la Universidad de Sevilla.

La promulgación reciente de la ley orgánica 5/92 sobre tratamiento automatizado de datos personales viene a cubrir un mandato constitucional cuya regulación no admitía más demora. La importancia de la materia ha suscitado, ciertamente, un amplio debate doctrinal en las etapas previas a la fase legislativa acerca de la conveniencia de un modelo u otro de regulación jurídica que no ha concluido, como era de esperar, con la aprobación y promulgación de la ley. Corresponde ahora a la doctrina y a quienes desde un sector u otro de la ciencia jurídica han manifestado su interés por esta materia realizar una labor rigurosa y depurada de crítica de las opciones que el legislador contempla en el texto de la ley.

Desde la promulgación de ésta no han cesado de publicarse trabajos que han analizado el contenido de sus preceptos, sus implicaciones y posibles consecuencias en la tutela del derecho a la intimidad, sus méritos y carencias y tantos otros aspectos que inciden o pueden incidir en la tutela efectiva de este derecho fundamental. Pero más allá de cuestiones concretas de su articulado, de la concordancia de la norma con otras del ordenamiento jurídico o de su relación con las distintas legislaciones nacionales sobre la materia e, incluso, su

concordancia con normas de derecho internacional, hay un aspecto que creo debe recabar nuestra atención y que suscita en quien esto escribe una perplejidad próxima al desaliento.

Y es que si algo puede provocar extrañeza en un lector mínimamente avisado es la falta de coherencia interna entre la exposición de motivos de la ley y el desarrollo pormenorizado de sus preceptos. Verdaderamente las declaraciones altisonantes y grandilocuentes de la parte expositiva pueden provocar una adhesión espontánea a sus proclamaciones que, a buen seguro, habrá de desvanecerse ineluctablemente tras una lectura crítica de sus contenidos normativos. Pareciera que ambas partes de la ley han sido redactadas por legisladores distintos con una diversa y muy distanciada concepción de los principios que deben inspirar la tutela de la intimidad frente al abuso informático.

Y esto nos aboca necesariamente a la cuestión de la coherencia interna del texto de la ley. La postura que aquí se sostendrá, en este sentido, pretende eludir valoraciones acerca de la conveniencia de opciones legislativas diversas de las adoptadas. Sencillamente,- estas líneas no permiten nada más-, intentaremos poner de manifiesto que lo que la LORTAD dice pretender no encuentra el reflejo correspondiente en su parte normativa, y a la inversa, los fines que esa parte normativa persigue poco tienen que ver con las declaraciones programáticas de su exposición de motivos. Y los que nos parece especialmente preocupante de todo esto no es ya las opciones y el modelo de tutela esbozado, sino la falta de coherencia interna de la ley. Se trata de una cuestión de técnica legislativa que dice muy poco del rigor jurídico de cuantos expertos han intervenido en la configuración del texto definitivo.

Nuestras observaciones habrán de verse necesariamente limitadas por lo estricto de una comunicación que pretende solamente poner de manifiesto una cuestión sobre la que quizás aún no se ha reparado suficientemente. En cualquier caso, el análisis de esta cuestión requerirá -si asumimos las consecuencias que de su planteamiento se derivan- un desarrollo ulterior y pormenorizado de los argumentos que en ella se esgrimen, pero creemos que existen razones que nos permiten mantener la conclusión aludida.

Veamos. Si algo puede resultar revelador en este sentido es la concepción que del derecho a la intimidad se deduce de la lectura de la exposición de motivos. Comienza nuestro legislador estableciendo una distinción entre privacidad e intimidad. La Constitución -nos dice- emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. Y miren ustedes por dónde, la preocupación que los redactores de la ley tienen ante las agresio-

nes a la intimidad por medios informáticos es tan acusada que no basta con establecer garantías eficaces -ésta y no otra es la característica definitoria esencial de la garantía- para defender la intimidad de los ciudadanos tal como viene entendida en el artículo 18 de nuestra norma suprema sino que la inquietud del legislador excede con mucho los límites constitucionales, es más podría uno pensar que la demora en atender el mandato constitucional del art. 18.4 responde a un proceso de maduración, de toma de conciencia por parte de quien tiene la difícil misión de garantizar el ejercicio de los derechos legítimos de los ciudadanos. Ya fuera de retardarse en su misión el legislador parece haber tomado buena nota de los acontecimientos y de las necesidades de tutela de la intimidad. No basta por tanto con establecer límites, con fijar garantías frente a las agresiones a la intimidad -entendida ésta en sentido estricto-, sino que existe un sector más amplio de la vida de los ciudadanos que debe ser adecuadamente protegido aún no perteneciendo propiamente a la esfera íntima:

"Nótese que se habla de la privacidad y no de la intimidad: Aquella 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..., 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."

Esta proclamación solemne con la que se inaugura la exposición de motivos parece dejar traslucir que la inquietud que el legislador tiene por asegurar la tutela efectiva de la privacidad es ciertamente importante. El objeto de la ley va más allá incluso, como hemos tenido ocasión de advertir, de la tutela estricta de la intimidad para penetrar en un ámbito más amplio de la vida de los individuos.Se trata de la privacidad, toda una amplia y heterogénea gama de conductas e informaciones sobre la vida de las personas que son susceptibles de defensa. El ámbito privado se define así por su carácter amplio y abierto y comprende todo aquello que en una u otra medida afecta a las peculiaridades de la persona en singular (honor, nombre, imagen, etc).

La agresión a través de medios informáticos puede afectar a datos relativos a ámbitos diferenciados de la vida de los individuos: vida familiar, profesional, relaciones personales, salud, creencias religiosas y políticas, hábitos de

vida, etc. Y el conocimiento de estas informaciones debe quedar lejos de alcance discrecional de quienes con finalidad lícita manipulan los ficheros automatizados.

Bien, hasta aquí el espíritu de la ley. Pero las intenciones de poco valen si no se adoptan medidas concretas tendentes a asegurar el respeto escrupuloso a la privacidad. Las proclamaciones solemnes pueden quedar en papel mojado si no se garantiza que eso que se proclama será efectivamente respetado. Y es aquí donde creemos que la ley hace aguas: las continuas excepciones en el régimen de ficheros públicos (artículos 21 y 22) pueden ser buen botón de muestra de cuanto decimos. La coherencia interna de la ley exige que se tomen medidas que garanticen lo que la ley proclama, o bien, si esto no puede ser así porque el legislador entiende que las exigencias de la sociedad informatizada no pueden quedar confinadas en los márgenes estrechos del respeto a la privacidad, que el texto de la ley no se adorne con la grandilocuencia de un discurso que no resistiría simple constatación de los hechos. Creemos que existen buenas razones para afirmar cuanto antecede, aunque no pretendemos hacer aquí un análisis exhaustivo del texto de la ley. Nos hemos referido a las abundantes excepciones que existen en materia de ficheros públicos, pero podríamos aludir también a la omisión del N.I.F. cuya regulación no ha sido expresamente contemplada por la ley y que alberga riesgos por todos conocidos, con carácter general podríamos mencionar igualmente las excepciones al principio del consentimiento contempladas en materia de cesión de datos -especialmente en lo relativo a datos recogidos de fuentes accesibles al público- (art.11.2), y con respecto a los ficheros de titularidad privada habría que referirse al insatisfactorio tratamiento de los datos relativos a la solvencia patrimonial y al crédito (art.28) y ficheros con fines de publicidad (art.29), sobre los que habría que hacer apreciaciones que exceden con mucho el objetivo de esta comunicación.

A todo ello habremos de añadir la pretendida independencia de la agencia de protección de datos que la ley instituye como garante de los derechos de los ciudadanos en materia de protección de datos. Resulta significativo el tenor de la exposición de motivos:

"La Agencia se caracteriza por la absoluta independencia del Director en el ejercicio de sus funciones, independencia que trae causa, en primer lugar, de un expreso imperativo legal, pero que se garantiza en todo caso, mediante el establecimiento de un mandato fijo que sólo puede ser acortado por un numerus clausus de causas de cese."

Una vez más hemos de manifestar nuestra sorpresa irrefrenable ante el tono de magnificencia y solemnidad de la exposición de motivos. Da la impre-

sión de que el título VI de la ley establece un órgano absolutamente independiente que ejerce sus funciones libre de toda atadura que pueda mermar efectivamente la tutela de los derechos de los ciudadanos. Pero esta inclinación desmedida por las frases grandilocuentes sitúa nuevamente a la ley en la encrucijada de su propia incoherencia. La historia nos ha enseñado suficientemente que las declaraciones solemnes de poco valen si no están sustentadas en garantías reales. Y es aquí donde surge el problema: el nombramiento y cese del Director de la Agencia depende del ejecutivo. De manera que ese criterio de "absoluta independencia" al que nos referimos es interpretado por el legislador en términos auténticamente insólitos.Y ello por dos motivos: primero, porque no nos parece que la independencia de que se nos habla quede asegurada en modo alguno ante la inminencia de un posible cese "por incumplimiento grave de sus obligaciones" que, en última instancia, es apreciado por el gobierno; segundo, porque nos provoca cierta incredulidad pensar que un órgano administrativo nombrado por el gobierno pueda ejercer un control efectivo sobre los bancos de datos de titularidad pública denunciando los desmanes que la Administración pudiera cometer.

Sin embargo, el legislador ha optado por un camino difícil. Es la vía de los grandes principios que luego se verán mermados no por una praxis errónea sino por una normativa carente de garantías. Lo que queda claro de todo ello es que la ley y la exposición de motivos discurren por senderos distintos y esto es lo que nos parece particularmente alarmante, sobre todo porque la opción por el respeto celoso de la privacidad podía haberse abandonado, sin olvidar la tutela de la intimidad, en beneficio del ejercicio legítimo del derecho a la información y de la transparencia informativa. Y da la impresión -un poco lastimosa- de que el legislador ha jugado con nuestra ingenuidad. Y es aquí donde todo esfuerzo exculpatorio pierde su sentido ante el reconocimiento incontestable y clamoroso de la incoherencia del legislador.

La Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal

MIGUEL LOPEZ-MUÑIZ GOÑI
Doctor en Derecho. Magistrado.

I. Introducción

El artículo 18.4 de la Constitución Española de 1978 dispone 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"*.

Con anterioridad a nuestra Constitución ya hubo borradores [1] y anteproyectos de normas. Ninguno de ellos llegó a plasmarse en un texto legal, pese a que en el Consejo de Europa se establecieron directrices generales, iniciadas desde la resolución del Comité de Ministros del Consejo de Europa de 26 de septiembre de 1973, sobre la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector privado, y la de 20 de septiembre de 1974, referente a los bancos de datos del sector público, y plas-

■ 1 Por Presidencia del Gobierno fue creada una Comisión de Expertos en 1972, que durante dos años estuvo trabajando en la redacción de un borrador de Ley de Protección de Datos. El autor de estas líneas formó parte de esta Comisión, dirigida por el Subdirector General de Informática Juan José Scala Estadella.

madas en el Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, y que fue ratificado por España el 31 de enero de 1982, publicado en el Boletín Oficial del Estado de 15 de noviembre de 1985.

El primer comentario que sugiere el texto constitucional es el recelo que manifiesta frente a la informática, puesto que no utiliza el término "regulará", como hace en otros casos [2] sino que emplea el restrictivo "limitará" [3]. Sin embargo, cuando por fin se dicta una ley sobre este tema, se comprueba que realmente se está "regulando" la incidencia de la informática sobre el derecho a la intimidad de las personas físicas.

Han tenido que transcurrir catorce años antes de que los legisladores hayan abordado el tema. En cumplimiento del mandato constitucional, se ha promulgado la Ley Orgánica 5/1992 de 29 de octubre, publicada en el Boletín Oficial del Estado de 31 de octubre de 1992, sobre "regulación del tratamiento automatizado de los datos de carácter personal", título que realmente responde al pretendido fin de la Ley, pero que, como ya hemos indicado, no "limita", sino que en su propio nombre refleja la intención de regulación.

Es imposible, en los estrechos límites de un artículo de revista, tratar de hacer un comentario completo a toda la Ley. Por ello vamos a limitarnos al estudio de los conceptos generales, dejando para mejor ocasión las disposiciones sectoriales, los tipos de fichero, infracciones y sanciones, etc...

II. Normativa Complementaria

Hasta la publicación de esta Ley, existían otras normas de distinto rango que regulan aspectos parciales de la protección de la intimidad. Por ejemplo:

- 2 Por ejemplo:
  - Artículo 17.4: "La ley regulará un procedimiento de "habeas corpus"..."
  - Artículo 20.3: "La ley regulará la organización y control parlamentario de los medios de comunicación social..."
  - Artículo 24.2: "La ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos"
  - Artículo 32.2: "La ley regulará las formas de matrimonio..."
  - Artículo 35.2: "La ley regulará un estatuto de los trabajadores"
  - Artículo 36: "La ley regulará las peculiaridades propias del régimen jurídico de los Colegios Profesionales..."

  Etc, etc.
- 3 Ya traté de este tema en mi artículo "La informática y el derecho a la intimidad" publicado en la Revista VEINTIUNO, número 3, otoño de 1989, pág. 29 a 42.

1. Ley 62/1978, de 26 de diciembre, de protección jurisdiccional de los Derechos Fundamentales de la persona.

2. Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil de Derecho al Honor, a la Intimidad Personal y Familiar y a la propia imagen. En la disposición transitoria 1ª de esta Ley se establece que *"en tanto no se promulgue la normativa prevista en el artículo 18.4 de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática, se regulará por la presente Ley"*.

3. Orden de 30 de julio de 1982 sobre limitación de acceso a la información contenida en las bases de datos fiscales.

4. Ley Orgánica 3/1985, de 29 de mayo, sobre modificación de la Ley Orgánica 1/1982, de 5 de mayo.

5. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, y ratificado por España, habiendo sido publicado en el Boletín Oficial del Estado de 15 de noviembre de 1985.

6. Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de salud pública.

7. Ley 14/1986, de 25 de abril, general de sanidad.

8. Ley 12/1989, de 9 de mayo, de la función estadística pública.

III. Estructura de la Ley

La Ley Orgánica 5/1992, sobre regulación del tratamiento automatizado de los datos de carácter personal, contiene un total de 48 artículos, tres disposiciones adicionales, una transitoria, una derogatoria y cuatro finales, respondiendo a la siguiente estructura:

- Una amplísima Exposición de Motivos, que analizaremos someramente.
- Título I, sobre Disposiciones generales.
- Título II, sobre principios de la protección de datos.
- Título III, sobre derechos de las personas.
- Título IV, Disposiciones sectoriales, con dos capítulos relativos a los ficheros de titularidad pública y privada.

- Título V, sobre movimiento internacional de datos.
- Título VI, sobre la Agencia de Protección de Datos.
- Título VII, sobre infracciones y sanciones.

Por razones de espacio sólo vamos a ocuparnos de la exposición de motivos y de los tres primeros títulos.

IV. La Exposición de Motivos

Resulta un tanto anómalo que una Ley de 48 artículos sea precedida por una Exposición de Motivos de casi tanta longitud como el articulado. Da la impresión de que han sido dos los redactores del texto legal, y que el autor del Preámbulo ha tratado de justificar o explicar algunos de los conceptos utilizados en el texto positivo, incluso habiéndose producido diferencias notables entre uno y otro.

1. Léxico utilizado.

El texto de una ley ha de ser lo suficientemente claro como para que todo el pueblo pueda entenderla, sin necesidad de acudir al Diccionario de la Real Academia de la Lengua. Es cierto que muchas veces han de utilizarse palabras técnicas, propias del lenguaje jurídico o de cualquier actividad, ciencia o parte que deba ser regulada, pero lo importante es que el ciudadano pueda captar la idea de lo que se le prohibe, ya que todo lo demás estará permitido.

No es que pretenda adentrarme en los complejos conceptos del uso del lenguaje legal, ya que otros muy ilustres profesores lo han tratado [4], pero sí creo interesante analizar algunos de los vocablos utilizados tanto en la prolija y larguísima Exposición de Motivos, como en algunos de los artículos del texto legal.

Por ejemplo, ya en el primer párrafo del apartado 1 se dice que la Constitución ha articulado "garantías contra la posible utilización torticera de ese fenómeno de la contemporaneidad que es la informática".

■ 4 Citamos, por ejemplo, a Antonio HERNANDEZ GIL, en su obra "El lenguaje jurídico", Juan Ramón CAPELLA, "El Derecho como lenguaje", Rafael BIELSA "Los conceptos jurídicos y su terminología", Cesáreo RODRIGUEZ AGUILERA, "El lenguaje jurídico", etc. Igualmente pueden verse mis trabajos "Problemática lingüística de los lenguajes especializados y técnicos", en el Ciclo "Informática y Lingüística". Madrid, noviembre de 1976; "Problemas lingüísticos de los bancos de datos", I Curso de Teledocumentación del Centro de Estudios Bibliográficos y Documentarios, Madrid, 1980; "La informática aplicada al lenguaje jurídico", Curso sobre Informática Jurídica, Facultad de Informática, 1981, etc.

Muchos conocen que la palabra "torticero" es equivalente a injusto, o que no se arregla a las leyes o a la razón; y también está admitido el vocablo "contemporaneidad", como calidad de contemporáneo; pero no deja de resultar anómala la rebuscada frase, cuando hubiera sido mucho más comprensible decir "el fenómeno contemporáneo" o actual.

En el tercer párrafo de este apartado 1 se utiliza la frase... " el tiempo...procuraba, con su transcurso, que se evanescieran los recuerdos..." El verbo "evanescer" equivale a desvanecer o esfumar, y tampoco es muy usado.

En el apartado 7 se utiliza la palabra "correlato" [5], cuando el Diccionario de la Real Academia ya indica que es un adjetivo de uso anticuado, debiendo utilizarse "correlativo". Pero si este adjetivo significa que sigue inmediatamente, no parece ser éste el sentido con el que se utiliza en el preámbulo de la Ley, sino que más bien debiera utilizarse la palabra "consecuencia", salvo que se pretenda seguir la doctrina de T.S. Eliot [6] en la crítica literaria.

2. Imprecisiones técnicas

A) Intimidad y privacidad.

El segundo párrafo del apartado 1 de la Exposición de Motivos dice textualmente lo siguiente: *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 se 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 menoscaba por la utilización de las tecnologías informáticas de tan reciente desarrollo.*

■ 5 "Sí se atribuye, sin embargo, a la Administración la potestad sancionadora que es lógico correlato de su función de inspección del uso de los ficheros, ..."

■ 6 T.S. ELIOT, "Hamlet and His Problems". 1919.

Los anglosajones han consagrado el vocablo "privacy", en un doble sentido, informático y de derecho subjetivo. En el primer sentido es definida en el Diccionario Oxford de Informática[7] como "protección que se establece para evitar la lectura de datos no autorizada". Y añade: "1. La protección de la información sobre un individuo o una entidad, cuando se determina que los datos se refieren a una persona específica, o en algunos casos a una organización específica, puede haber un derecho legal a limitar el acceso a esa información y, en muchos casos, pueden existir derechos asociados que garanticen la exactitud y exhaustividad de dichos datos. Esta forma de protección de la intimidad se establece, únicamente, para la información sobre un individuo identificable y para salvaguardar los derechos del individuo al que pertenecen los datos".

En el sentido del derecho subjetivo, ya fue formulado por Warre y Brandeis [8] como el derecho de ser dejado a solas. Pero en España se utiliza el término "intimidad", del que ya nos ocupamos en otro lugar [9]. Los redactores de la Exposición de Motivos pretenden realizar una diferenciación entre "privacidad", considerándola como el conjunto de elementos que, separadamente no son transcendentes, pero una vez correlacionados, pueden producir perjuicio a una persona, mientras que la "intimidad" se refiere "a las facetas más singularmente reservadas de la vida de la persona", según frase de la Ley.

No estamos, en absoluto, de acuerdo con esta diferenciación. Como dice Georgina Batlle [10], la intimidad es "el derecho que compete a toda persona a tener una esfera reservada en la cual desenvolver su vida sin que la indiscreción ajena tenga acceso a ella". De ahí que muchos datos personales pueden tener el carácter de íntimos para unas personas y carecer de tal para otras. El domicilio e incluso el teléfono, pueden llegar a ser "datos sensibles", que son todos aquellos que se refieren a cuestiones que el interesado pretende reservar para sí, en todo momento o en uno determinado. Sin embargo, las opiniones políticas o religiosas pueden ser tan públicas que carezcan del concepto de datos íntimos o reservados.

- 7 "Diccionario Oxford de Informática". 1ª Edición. Díaz de Santos. Traducción de Blanca de MENDIZABAL ALIENDE.
- 8 Warre y Brandeis. "The right to privacy". Harvard Law Review. Vol. 4. 1890.
- 9 Véase nuestro artículo "La Informática y el Derecho a la intimidad", publicado en el número 3 de esta misma Revista VEINTIUNO, en otoño de 1989.
- 10 Georgina BATLLE. "El derecho a la intimidad privada y su protección". Editorial Alfil. Alcoy, 1972.

Los datos son íntimos, privados en su sentido de lo que es propio de cada uno, y solamente cada ciudadano debe señalar cuáles son aquellos que estima no deben trascender a los terceros. Un comerciante puede tener gran interés en que su domicilio y teléfono aparezca no sólo en la guía de este servicio, sino todos los días en la prensa, mientras que un Magistrado o un Policía quieren tenerlos reservados de la curiosidad pública.

Es cierto que la intimidad personal y familiar está protegida en el primer párrafo del artículo 18 de la Constitución, complementado con la inviolabilidad del domicilio y del secreto de la correspondencia. Pero esta referencia a la protección de la intimidad es la que, precisamente, hace que se limite el uso de la informática. Cualquier nuevo concepto que se pretende introducir a través de la Exposición de Motivos resulta inadecuado, sobre todo cuando a lo largo del texto legal no se vuelve a utilizar el término de "privacidad". Es más, el artículo primero de la Ley establece que se trata de "garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos". Por lo tanto, la referencia a la privacidad de la Exposición de Motivos es supérflua e innecesaria.

El español es lo suficientemente rico como para que el concepto de "intimidad" permita su aplicación a los datos sensibles, sin necesidad de acudir a "préstamos lingüísticos", a los que tan aficionados somos cuando se trata de terminología técnica, por su difícil transposición de los consagrados internacionalmente, como ocurre con los ya tan manoseados software y hardware. Establecer una artificial diferenciación entre intimidad y privacidad sólamente por el tratamiento informatizado de los datos, o su posible correlación, no conduce a parte alguna.

Los datos de una persona tienen el carácter de sensibles en razón y fundamento de esa misma persona, de su titular, que es el único que debe manifestar si los mismos pueden ser incorporados o no a los ficheros informatizados, ya sean éstos autónomos o interrelacionados.

B) Ficheros o bancos de datos personales.

Aparece en la Exposición de Motivos un aspecto técnico muy curioso e interesante. Se habla, a través de toda la Ley Orgánica, de "ficheros de datos", en torno a los cuales "se nuclea" (sic) [11] la misma.

■ 11 "Nuclear" es lo relativo o perteneciente al núcleo. La Real Academia de la Lengua Española no reconoce la existencia del verbo "nuclear", del que se conjugaría "nuclea", utilizado en esta Ley, como centrar.

Fichero, en sentido informático, es una colección de datos, o conjunto de registros relacionados tratados de la misma manera. Base de datos es la integración de ficheros, de tal forma que cualquiera de sus datos pueda utilizarse como información clave para especificar consultas. De ahí que técnicamente debiera haberse utilizado el término "bases de datos" y no el más restringido de ficheros de datos. Unicamente en el caso de que se piense que los datos de un fichero pueden ser sensibles sólamente cuando se relacionan con otros (la privacidad de la que habla la exposición de motivos), en cuyo caso la posibilidad de acceso por elementos no previstos, o su puesta en relación con otros que figuren en diferentes ficheros, producen la "combinación diabólica" no prevista ni querida por el creador del primero de aquéllos.

Precisamente por esta deficiencia terminológica, el párrafo segundo del apartado 2 de la Exposición de Motivos dice que *"a tal efecto, la Ley introduce el concepto de tratamiento de datos, concibiendo los ficheros desde una perspectiva dinámica: dicho en otros términos, no los entiende sólo como un mero depósito de datos, sino también, y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el perfil personal al que antes se hizo referencia"*. Nuevamente aparece la disociación entre el redactor de la Exposición de Motivos y el texto articulado, al insistir aquí en el concepto de privacidad como un aspecto informático de la intimidad, a lo que nos oponemos por razones tanto lingüísticas como jurídicas.

Ahora bien, si se trata de una legislación técnica, sobran las explicaciones en la exposición de motivos, bastando con el artículo dedicado a las definiciones. No se trata de explicar toda la teoría informática, sino de regular los procesos que pueden afectar a los datos personales. El artículo 3.b) de la Ley, efectivamente, define lo que es un fichero informatizado, diciendo que es *"todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso"*. Echamos en falta que en el título de esta definición no se haya utilizado el concepto de "fichero informatizado de datos personales", que es, en realidad, a lo que se refiere el texto legal, criterio que salva el propio artículo 3º al decir que esta definición es "a los efectos de la presente Ley".

C) Datos anónimos.

El quinto párrafo del apartado 2 de la Exposición de Motivos manifiesta que quedan fuera del ámbito de aplicación de la Ley los datos anónimos, *"que constituyen información de dominio público o recogen información, con la finalidad,*

precisamente, de darla a conocer al público en general", poniendo como ejemplo los Registros de la Propiedad y Mercantiles. La redacción es defectuosa, puesto que parece que los datos de estos registros son de carácter anónimo, cuando claro es que no es así, por lo que debiera haberse redactado en el sentido de que quedan fuera del ámbito de aplicación de la Ley los datos anónimos, que constituyen información de dominio público, "y aquellos otros que recogen información con la finalidad, precisamente, de darla a conocer al público en general". Es importante el uso de la conjunción copulativa en lugar de la disyuntiva.

V. El Título I. Disposiciones Generales

Se refiere a las disposiciones generales, diciéndose en la Exposición de motivos que *"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 la racionalidad de la utilización de los datos. Este principio, verdaderamente cardinal, de la congruencia y la racionalidad, garantiza que los datos no puedan ser usados sino cuando lo justifique la finalidad para la que han sido recabados; su observancia es, por ello, capital para evitar la difusión incontrolada de la información que, siguiendo el mandato constitucional, se pretende limitar".*

1. Objeto de la Ley.

Se refiere el artículo 1 que el objeto de la Ley es *"limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos".*

Esta protección se extiende no solamente a los bancos de datos personales establecidos en España, sino también a la circulación transfronteras de los datos, conforme lo establecido en el título V, exigiendo que los países receptores dispongan también de normas que protejan la intimidad de forma equivalente.

2. Ambito de la Ley.

En el artículo 2 establece que la Ley *"será de aplicación a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado".*

Sin embargo, no será de aplicación en los supuestos siguientes:

a). A los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general.

b). A los ficheros mantenidos por personas físicas con fines exclusivamente personales.

c). A los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales.

d). A los ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos o repertorios oficiales.

Este apartado no recoge el caso de la jurisprudencia no publicada, o utilizada antes de que vea la luz en las Colecciones Oficiales, circunstancia que se da en la mayor parte de las bases de datos de jurisprudencia.

e). A los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex-miembros, sin perjuicio de la cesión de los datos que quede sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos.

De otra parte, quedan excluidos de esta Ley, y se regulan por sus disposiciones específicas:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los sometidos a la normativa sobre protección de materias clasificadas.

c) Los derivados del Registro Civil y del Registro Central de Penados y Rebeldes.

d) Los que sirvan a fines exclusivamente estadísticos y estén amparados por la Ley 12/1989, de 9 de mayo, de la función estadística pública, sin perjuicio de lo dispuesto en el artículo 36.

e) Los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el artículo 68 de la Ley 17/1989, de 19 de julio, Reguladora del Régimen del Personal Militar Profesional.

3. Definiciones.

El artículo 3º se dedica a las definiciones de lo que se consideran datos de carácter personal, fichero automatizado, tratamiento de datos, etc.

A) Fichero automatizado.

Ya hemos indicado que la Ley se refiere a ficheros automatizados, y no a bancos de datos, siendo por tanto más amplio su campo de aplicación, y protegiendo la intimidad incluso en aquellos supuestos en que no puedan extrapolarse los datos sensibles recogidos en ficheros específicos.

B) Responsable de un fichero.

Considera responsable del fichero a la *"persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento"*. No parece muy acertado el nombre de "responsable", siendo más adecuado el de "Administrador" del fichero o banco de datos, es decir, lo que los anglosajones denominan "data-processing manager", y que es definido [12]como el ejecutivo responsable de la función de proceso de datos en una organización, es decir, la persona que vela por la organización, planteamiento y dirección del servicio de proceso de datos, según las directrices establecidas por la dirección de la empresa.

C) Sujeto titular de los datos.

Define también este artículo quién es el "afectado", que no es otro que la *"persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo"*, es decir, aquél cuyos datos están sometidos a "operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación conservación, elaboración, modificación, bloqueo y cancelación así como las cesiones de datos que resulten de comunica-

■ 12 Véase el DICCIONARIO DE INFORMATICA OXFORD, 2ª edición. Madrid, 1992. Editorial Díaz de Santos. Traducción de Blanca DE MENDIZABAL ALIENDE.

ciones, consultas, interconexiones y transferencias." Nuestra Ley sigue en esto a la Ley Alemana de Protección de Datos de 27 de enero de 1977, que entiende por "afectado" la persona natural determinada o determinable cuyos datos de carácter personal o material se incluyen en un archivo informatizado.

Según el Diccionario de la Lengua Española, afectar significa, en su 5ª acepción, "atañer, tocar", y afectado, en su 4ª acepción, es el "aquejado, molesto, enfermo". Sin embargo, no parece ser ésta la mejor palabra que defina a la persona cuyos datos son objeto de registro en un fichero.

La Ley de Datos de Suecia de 11 de mayo de 1973, entiende por "persona registrada" la persona individual con relación a la cual existiere información personal en un archivo de personas. La Ley de Protección de Datos Personales de Austria, de 27 de julio de 1986, se refiere a "interesado". Y la ley de Protección de Datos del Reino Unido de 12 de junio de 1984 lo denomina "sujeto de datos" o "persona objeto de datos" al individuo que fuere titular de los datos personales que se incluyen en un fichero.

En nuestro ordenamiento jurídico es muy común el empleo de la palabra "sujeto", como por ejemplo, el sujeto pasivo de los impuestos, empleando este vocablo como uno de los elementos de una situación jurídica, como titular de un derecho, frente a los derechos sin sujeto. Igual que, según Capella [13], cada norma jurídica tiene un sujeto, los datos personales incluidos en un fichero o banco de datos también tienen sujetos titulares de dichos datos.

D) Procedimiento de disociación

Por último, se define lo que es el "Procedimiento de disociación": *"todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable"*. Esto hace que un dato sensible pierda tal carácter cuando es asociado a otros iguales, sin posible conexión con la persona a la que se refiere, es decir, está "disociado" de aquella; tal es el caso de los datos estadísticos. Los datos disociados pueden ser perfectamente tratados informáticamente, siempre que no se mantenga la relación con la persona concreta, debiendo mantenerse ambos ficheros por separado y sin conexión posible.

■ 13 Juan Ramón CAPELLA. "El Derecho como lenguaje". Ediciones Ariel. Barcelona, 1968.

VI. Títulos II y II. Los principios de la Protección de Datos

Los principios fundamentales de la protección de datos se agrupan en dos grandes apartados.

El primero de ellos es el grupo de derechos que corresponden al sujeto de datos, y que son los siguientes: a) el del consentimiento, previo a la incorporación a un fichero de los datos personales; b) el derecho de información, que corresponde al conocimiento de lo que realmente existe o se ha incorporado al fichero; c) el derecho de acceso, o comprobación por el interesado, de una forma periódica, de lo que se mantiene en el fichero; d) el derecho de rectificación, para que los datos incorporados a un fichero sean exactos; e) el derecho a la veracidad de los datos, es decir, que los de carácter personal incorporados a un fichero deben actualizarse para que permanezcan acordes con la realidad; f) el derecho de indemnización de los perjuicios que pueden ocasionarse por el uso indebido de la informática.

El segundo grupo es el conjunto de principios relacionados con el propio fichero que contiene los datos personales. Aquí podemos considerar: a) el principio de legalidad en la captación de datos; b) el principio de unicidad, o la necesidad de que los datos captados respondan a la finalidad del fichero, sin que puedan difundirse o tratarse fuera de esa finalidad; c) principio de la adecuación, según el cual los datos recogidos, serán los pertinentes y no excesivos, teniendo en cuenta la finalidad del fichero; d) el principio de caducidad, que exige que los datos incorporados a un fichero no se conservarán en el mismo más tiempo que el necesario para cumplir con su finalidad; e) el principio de seguridad, tanto informática como general, para garantizar la conservación de los datos y la no revelación de los mismos salvo dentro de la finalidad del fichero.

Veámos cómo estos derechos y principios son tratados en la Ley.

VII. Derechos del Sujeto de los Datos

1. Derecho a prestar el consentimiento.

El principio del consentimiento exige que el sujeto de datos manifieste expresamente su conformidad en que los que le afecten sean incorporados al fichero correspondiente.

El artículo 6 de la Ley [14] exige el consentimiento del afectado o sujeto de los datos, para que aquéllos que a él se refieren puedan ser incorporados a un fichero o base de datos. Este consentimiento es revocable, aunque la misma no tendrá carácter retroactivo.

Este precepto se complementa con lo dispuesto en el artículo 7 [15] que bajo la rúbrica de "Datos especialmente protegidos" establece que nadie puede ser obligado a declarar sobre su ideología, religión o creencias, conforme lo dispuesto en el artículo 16 de la Constitución.

Si alguien no tiene inconveniente en que estos datos figuren en un fichero informatizado debe dar su consentimiento expreso y por escrito.

De cara a los futuros ficheros, la norma es perfectamente aplicable, pero nada se establece en las disposiciones adicionales ni transitorias sobre aquellos ficheros establecidos con anterioridad a la entrada en vigor de la Ley, y que contienen este tipo de datos especialmente protegidos, aunque, por lógica, el Responsable del fichero deberá solicitar la autorización a todas las personas que figuren en el mismo, cumpliendo con los requisitos establecidos en el artículo 5.1.

2. Derecho de información.

Complemento del principio del previo consentimiento está el principio de información, que exige que el "afectado" o sujeto de los datos sea informa-

■ 14). - Artículo 6. Consentimiento del afectado.

1.- El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa.

2.- No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

3.- El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuya efectos retroactivos.

■ 15).- Artículo 7.

1.- De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2.- Sólo con consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento automatizado los datos de carácter personal que revelen la ideología, religión y creencias.

do periódicamente, sin retrasos ni gastos, de los datos personales que le afecten, pudiendo acceder a los mismos en la forma y manera que legalmente se establezca.

Este principio se recoge en el artículo 5 de la Ley, obligando al Responsable del fichero a informar, de forma expresa, precisa e inequívoca, a los sujetos de datos personales, de la existencia del fichero, la finalidad de la recogida de los datos y los destinatarios de la información; la obligatoriedad o no de facilitar la respuesta; las consecuencias de la obtención de los datos o de la negativa a suministrarlos; la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, y de la identidad y dirección del responsable del fichero.

No parece muy lógica la salvedad de facilitar esta información prevista en el artículo 5.3, que dice que *"si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban"*, puesto que queda el derecho de información supeditado a la interpretación del responsable del fichero, que siempre podrá alegar que la finalidad del mismo se deducía de las preguntas formuladas. Es, sin duda, este apartado, uno de los que más problemas prácticos puede presentar. De ahí que Diego López Garrido [16] haya hablado de que este precepto es inconstitucional.

Además, existe una clara contradicción entre ambos preceptos: Por un lado, la obligación de recabar el consentimiento del afectado en todos los casos en que vayan a tratarse automáticamente datos de carácter personal; y por otro, la falta de información sobre la existencia del propio fichero, las consecuencias del tratamiento, o el derecho de acceso, rectificación y cancelación. Parece que estima debe prevalecer el derecho a tratar datos personales sobre el de protección de la intimidad, cuando constitucionalmente es la inversa.

Por último, el artículo 13 regula el Derecho de información, de la siguiente forma: *"Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de ficheros automatizados de datos de carácter general, sus finalidades y la identidad del responsable del fichero. El Registro General será de consulta pública y gratuíta"*.

Sin embargo, este derecho de información no es el adecuado, puesto que lo único que se concede es la facultad de conocer qué ficheros existen, pero no

■ 16).- Diego LOPEZ GARRIDO.- "Informe de la Comisión de Libertades Públicas e Informática". (CLI).

en cuáles se encuentra registrado el interesado y los datos que del mismo se contienen en cada uno. Este principio de información queda en la Ley sustituido, en este sentido, por el derecho de acceso, confundiendo ambos.

Resulta anómalo que un sujeto de datos deba acceder a todos los posibles ficheros informatizados para conocer si está o no incluido en los mismos, y cuáles datos son los que allí figuran y que le afectan.

El problema no debe existir en relación con los ficheros posteriores a la Ley, ya que será preciso el previo consentimiento; pero no quedan resueltas las cuestiones relacionadas con los ficheros previos a la entrada en vigor de la Ley, desconociendo el ciudadano si se encuentra o no en ellos, puesto que lo establecido en la disposición adicional segunda, referente a la comunicación a la Agencia de Protección de Datos de los ficheros existentes con anterioridad, no dice nada sobre la información de los afectados.

3. Derecho de acceso.

Junto al derecho de información existe el de acceso, confirmado en el artículo 4.6, que dice que los datos personales *"serán almacenados de forma que permitan el ejercicio del derecho de acceso por parte del afectado", insistiendo en la existencia de tal derecho en el artículo 5.d).*

El artículo 14 es el que regula de forma específica el derecho de acceso[17], logrando el mismo mediante consulta directa al fichero, o bien solicitando copia de los registros que afecten al interesado, pudiendo realizar esta consulta cada año.

4. Derecho de rectificación.

Todo sujeto de datos personales tiene derecho a que los mismos sean corregidos cuando contengan errores, inexactitudes, o los mismos no sean adecuados a la finalidad del fichero donde se encuentran.

■ 17).- Artículo 14. Derecho de acceso.

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 doce meses, salvo que el afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.*

El artículo 5.1.d) reconoce el derecho de rectificación de los datos, estableciendo el artículo 4.4 que *"Si los datos de carácter personal registrados resultaran ser inexactos en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 15"*.

Dos aspectos presenta este artículo. De una parte, el hecho de que este precepto esté incardinado dentro de la rúbrica referente a la calidad de los datos, y por lo tanto, ha de deducirse que la inexactitud total o parcial, siendo ésta por error o por defecto, se ha detectado por parte del propio Administrador o Responsable del fichero, en cuyo caso es él mismo quien debe proceder a la rectificación. Esto mismo se deduce de la propia referencia de este precepto al derecho de rectificación previsto en el artículo 15.

De otra parte, es anómalo el uso de frase "serán cancelados", puesto que cancelar es la supresión o anulación de un registro , y aquí no se trata de la supresión definitiva del dato erróneo, sino su sustitución por el dato verdadero. Por ello, parece más lógico que la frase hubiera quedado en la siguiente forma: "inexactos en todo o en parte, o incompletos, serán sustituidos por los correspondientes datos rectificados o completados".

El citado artículo 15 se refiere al Derecho de rectificación y cancelación [18] , es decir, la posibilidad de que el interesado solicite la rectificación de sus datos personales que figuran en un registro, o bien que sean borrados del mismo bien porque ya han dejado de ser ciertos, bien porque revoca su autorización para que sean incorporados al fichero.

Según este precepto, se deja para su regulación reglamentaria el trámite para ejercer el derecho de rectificación, o cancelación en su caso, así como el plazo para que la corrección se lleve a efecto.

En el número 2 ya se corrige la antinomia entre cancelación y rectificación, señalada respecto del artículo 5.1.d), puesto que se habla de rectificación

■ 18).- Artículo 15. Derecho de rectificación y cancelación.

1.- 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.

2.- Los datos de carácter personal que resulten inexactos o incompletos serán rectificados y cancelados en su caso.

3.- Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario.

4.- La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos.

5.- 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 fichero y el afectado.

de los datos erróneos o incompletos, y cancelación, en los supuestos de denegación del consentimiento, o de tratarse de datos especialmente protegidos de los regulados en el artículo 7, sin haber obtenido el previo consentimiento expreso y por escrito.

5. Derecho a indemnización.

Siempre que existe una actuación ilegal o ilícita, así como cuando por acción u omisión se causa daño a otro, interviniendo culpa o negligencia, debe darse lugar a la indemnización de daños y perjuicios.

Por ello, en la Ley de Protección de Datos se prevé esta posibilidad en su artículo 17 [19] que nace ya bajo la duda de su inconstitucionalidad.

Así, López Garrido [20] considera que el dejar para un Reglamento la regulación de la forma de reclamación contra las actuaciones contrarias a lo dispuesto en la Ley, va contra el principio constitucional de legalidad establecido en el artículo 25.1 de nuestra Constitución, que exige que las sanciones administrativas tienen que estar previstas por una Ley. El hecho de que en esta Ley Orgánica se establezcan las infracciones y sanciones no permite que en un Reglamento se establezca la forma de ejercer la reclamación.

Hay que hacer notar la defectuosa redacción del apartado 3 de este artículo 17, cuyo contenido quedaría mucho más claro si dijera que "Tendrán derecho a ser indemnizados los afectados que sufran daño o lesión en sus bienes o derechos como consecuencia del incumplimiento, por el responsable del fichero, de lo dispuesto en la presente Ley."

Es indudable que la inclusión de este precepto puede aclarar un derecho que ya se tiene reconocido tanto por el artículo 1902 del Código Civil como por el principio de responsabilidad del Estado en el supuesto de tratarse de ficheros públicos.

■ 19).- Artículo 17.- Tutela de los derechos y deberes de indemnización.

1.- Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los afectados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2.- Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

3.- Los afectados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable del fichero, sufran daño o lesión en sus bienes o derechos, tendrán derecho a ser indemnizados.

4.- Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

5.- En el caso de los ficheros de titularidad privada la ación se ejercitará ante los órganos de la jurisdicción ordinaria.

■ 20).- Diego López Garrido. Informe de la Comisión de Libertades Públicas e Informática (CLI).

El texto legal considera necesario explicar que la responsabilidad, en el caso de ficheros públicos, se exigirá ante las Autoridades Administrativas, y el consiguiente recurso contencioso-administrativo, mientras que cuando se trata de ficheros privados debe exigirse la responsabilidad ante la jurisdicción ordinaria.

VIII. Principios Relacionados con el propio Fichero

1. Principio de adecuación.

Los datos que se recojan para ser incorporados a ficheros informatizados han de ser los adecuados y pertinentes, en relación con la finalidad pretendida por el fichero. Además no han de ser excesivos, evitando la recogida de datos complementarios que puedan afectar a otras áreas de la intimidad de la persona. Al mismo tiempo, estos datos no podrán ser utilizados para una finalidad diferente de la pretendida.

El artículo 4 de la Ley, y bajo la rúbrica de "calidad de los datos", hace referencia a este principio de adecuación, estableciendo que *"sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido"*.

Lo que ya no parece tan posible es la limitación de la Ley de que en *"su clasificación sólo podrán utilizarse criterios que no se presten a prácticas ilícitas"*, ya que una características del tratamiento informático es la posibilidad de buscar y clasificar los datos de una forma aleatoria, incluso aun cuando los sistemas de acceso o recuperación hayan sido fijados de antemano.

Es de esperar que reglamentariamente se establezca qué criterios van a imponerse en este terreno, ya que es lógico pensar que deban especificarse los campos que compongan cada registro, y cuáles de ellos van a ser los que sirvan como elemento de recuperación. Igualmente se espera que deberán constar en la Agencia de Protección de Datos los sistemas informáticos de recuperación de la información.

2. Principio de veracidad.

Los datos personales incorporados a un fichero informatizado serán exactos, debiendo actualizarse siempre que sea preciso. El artículo 4.3. exige la

exactitud de los datos personales diciendo que dichos datos *"serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado".*

Este principio es el correlativo con el derecho de rectificación, puesto que lo que se trata es de que los datos contenidos en el fichero coincidan lo más exactamente posible con la realidad.

3. Principio de legalidad en la captación de datos.

Los datos personales que se incorporen a un fichero informatizado será obtenida y procesada de forma legal.

El artículo 4.7 establece que *"se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos."*

La Ley, en su artículo 7, apartados 4 y 5, y bajo la rúbrica general de "Datos especialmente protegidos", establece lo siguiente:

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, religión, creencias, origen racial o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros automatizados de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Igualmente queda restringida la captación de datos en materia de sanidad y salud, a los que se refiere el artículo 8 [21] .

4. Principio de unicidad.

Los datos personales sólo serán guardados en ficheros informatizados, para la finalidad prevista para los mismos. Igualmente, la utilización, revelación o difusión de los datos no será incompatible con esa finalidad.

■ 21 Artículo 8. Datos relativos a la salud.
Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento automatizado de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en los artículos 8, 10, 23 y 61 de la Ley 14/1986, de 25 de abril, General de Sanidad; 85.5 y 96 de la Ley 25/1990, de 20 de diciembre, del Medicamento; 2, 3 y 4 de la Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de Salud Pública y demás Leyes sanitarias.

Esto exige que la finalidad del fichero que contenga datos personales quede perfectamente definida desde el primer momento, justificándose así la necesidad de obtener y procesar este tipo de datos sensibles.

El artículo 4.2 de la Ley dice que *"los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos"*.

Por esa misma razón, se prohíbe la cesión de los datos para que sean tratados, incorporados a otros ficheros, o difundidos por diferentes medios para los cuales fueron captados.

El artículo 11 de la Ley [22] regula la cesión de datos siguiendo el principio general de la prohibición, salvo caso expreso de consentimiento por parte del interesado, y siempre será revocable.

El criterio general es que los datos van a ser tratados y difundidos en y desde el fichero para el cual han sido captados y autorizados, y sobre el que el sujeto de datos ha ejercido sus derechos de consentimiento, información y rectificación. De ahí que este artículo 11.1 exija el previo consentimiento del afectado, antes de que se produzca la transferencia o cesión de los datos, con el fin de que aquel pueda ejercitar igualmente sobre el nuevo fichero, los derechos de información y rectificación.

■ 22 Artículo 11. Cesión de datos.

1. Los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando una Ley prevea otra cosa.

b) Cuando se trata de datos recogidos de fuentes accesibles al público.

c) Cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros. En este caso sólo será legítima en cuanto se límite a la finalidad que la justifique.

d) Cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tienen atribuidas.

e) Cuando la cesión se produzca entre las Administraciones Públicas en los supuestos previstos en el artículo 19.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado o para realizar los estudios epidemiológicos en los términos establecidos en el artículo 8 de la Ley 14/1986, de 25 de abril, General de Sanidad.

3. Será nulo el consentimiento cuando no recaiga sobre un cesionario determinado o determinable, o si no constase con claridad la finalidad de la cesión que se consiente.

4. El consentimiento para la cesión de datos de carácter personal tienen también un carácter de revocable.

5. El cesionario de los datos de carácter personal se obliga, por el solo hecho dé la cesión, a la observancia de las disposiciones de la presente Ley.

6. Si la cesión se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Por eso mismo el número 3 de este artículo establece la nulidad del consentimiento cuando no recaiga sobre un cesionario determinado o determinable, es decir, sobre un fichero cuyas características puedan conocerse, tanto en cuanto la finalidad del mismo, como en relación con los datos recogidos. Igualmente se exige por la Ley que el Responsable del fichero que va a ceder los datos personales ponga de manifiesto, de una manera clara y diáfana, al afectado la finalidad de la cesión que se solicita, con el fin de que el sujeto de datos pueda prestar su consentimiento de una manera consciente y responsable.

Creemos que está mal redactado el número 4, cuando declara que el consentimiento para la cesión de datos personales "tiene un carácter de revocable". Lógicamente debiera decir "el carácter", o simplemente prescindir del artículo. La redacción actual no tiene sentido.

El último párrafo, el 6º, determina que no es necesario el consentimiento si la cesión se efectúa previo procedimiento de disociación, es decir, rompiendo la relación entre el dato y su sujeto, para quedar el primero integrado o asociado a otros, figurando a partir de ese momento con carácter anónimo.

5. Principio de caducidad

Los datos personales incorporados a un fichero no se mantendrán en el mismo más tiempo que el necesario para cumplir esa finalidad. La cancelación, pues, es equivalente a borrar, anular o hacer ineficaz de forma permanente, un registro de un fichero.

Los ficheros informatizados pueden encontrarse "on line", es decir, preparados para que se pueda acceder a ellos en cualquier momento, o bien "off line", es decir, fuera de línea; y en este caso, pueden encontrarse sobre soportes magnéticos en forma de backup, o copia de seguridad.

El artículo 4.5 [23] regula la cancelación de los datos cuando ya no sean necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.

■ 23 Artículo 4, apartado 5:
Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.
No serán conservados de forma que permitan la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.
Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos sus valores históricos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

Debe entenderse que los datos personales deben de estar situados "on line" en el momento mismo en que dejan de ser necesarios para la finalidad para la que han sido captados y registrados, pudiendo existir en cualquier momento las copias de seguridad necesarias. Una vez que la finalidad del fichero se ha cumplido, y los datos almacenados dejan de ser necesarios, no sólamente han de ser suprimidos de los sistemas de trabajo normales, sino también deben quedar destruidas las copias de seguridad, a partir de las cuales podrían regenerarse los ficheros.

Puede llevarse a cabo la conservación de los datos de una forma disociada, es decir, sin que queden unidos a su titular; por ejemplo, de una manera estadística.

6. Principio de seguridad

Según el Principio de seguridad, el Administrador o Responsable del fichero ha de adoptar las medidas de seguridad, tanto generales como informáticas, para proteger los datos personales del acceso a los mismos, su modificación la revelación o la destrucción, por personas no autorizadas para ello, así como para evitar la destrucción o la pérdida que se produzca accidentalmente.

Este principio está recogido en el artículo 9 [24].

Las medidas de seguridad pueden ser de dos clases: protección del acceso al local u oficina donde se encuentra el ordenador; y la protección de los datos. En el primer sentido, deben considerarse todas las medidas de vigilancia de carácter general, de tal forma que se impida el acceso al local de aquellas personas no autorizadas y que, de forma intencionada o no, acceder a los datos o alterarlos. De ahí lo establecido en el último inciso del apartado 2°.

En el segundo sentido, se refiere a la protección de los datos frente al acceso a la información por parte de persona no autorizada, o la destrucción o

■ 24 Artículo 9. Seguridad de los datos.

1. El responsable del fichero deberá adoptar las medidas de índole técnica y organizativa 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 ao del medio físico natural.

2. No se registrarán datos de carácter personal en ficheros automatizados 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 automatizados y las personas que intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de este Ley.

alteración de los mismos de una forma intencionada, pero no autorizada por el responsable del fichero. Para lograr esta seguridad se establecen limitaciones lógicas o físicas para poder acceder a todos los ficheros, o bien a los elementos más sensibles de los mismos.

Es lógico que el artículo 9.3 exija unas determinadas condiciones de seguridad para la protección de los datos especialmente protegidos, a los que se refiere el artículo 7, es decir, ideología, religión o creencias.

7. Principio de secreto profesional.

Aquellas personas que trabajan en ficheros que contienen datos personales están obligadas al secreto profesional. Así lo recogen las Normas Básicas de Deontología Informática [25] diciendo que *"el informático no difundirá ni comunicará a terceras personas datos de carácter personal o íntimo registrados en bases o bancos de datos a los cuales tuviere acceso en el ejercicio de su actividad. Sólo facilitará datos de carácter personal o íntimo cuando en virtud de disposiciones legales fundadas en el Bien Común o el interés público estuviere obligado a ello".*

El artículo 10 de la Ley establece este deber de secreto, diciendo que *"El responsable del fichero automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlo, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo".*

Como es natural, la violación del secreto se considera falta grave, e incluso falta muy grave cuando se trata de datos especialmente protegidos (ideología, religión o creencias, y origen racial, salud y vida sexual).

■ 25 "Normas básicas de Deontología Informática". Redactadas por el Grupo de investigación de CITEMA, integrado por José Carlos-Roca, Manuel Heredero Higueras, Luis Navarro Gil y Ramón Villanueva Etcheverría.

La Regulación de los Datos Sensibles en la LORTAD

ALVARO A. SÁNCHEZ BRAVO

Profesor-Colaborador del Departamento de Filosofía del Derecho, Moral y Política. Facultad de Derecho. Universidad de Sevilla.

SUMARIO

INTRODUCCION

CONCEPTUACION DE LOS DATOS SENSIBLES

DETERMINACION DE LOS DATOS SENSIBLES: SU DINAMICIDAD

¿NUMEROS CLAUSUS O NUMEROS APERTUS?

REGULACION DE LOS DATOS SENSIBLES EN LA LORTAD:

A) Determinación de los Datos Sensibles
B) Enumeración y Contenido
C) Régimen Jurídico

D) Excepciones a la prohibición de tratamiento de datos sensibles: Ficheros de las Fuerzas y Cuerpos de Seguridad.

ULTIMAS CONSIDERACIONES. A MODO DE CONCLUSION

Introducción

La existencia en las legislaciones nacionales de una ley sobre tutela de los datos personales es una importante garantía de las libertades fundamentales del ciudadano [1].

Con la introducción de las nuevas tecnologías de tratamiento automatizado de los datos es cuando se ha manifestado la potencialidad lesiva ya presente en la recogida, múltiple, masiva e indiferenciada, de los datos personales [2].

En nuestro país la promulgación de la L.O.R.T.A.D.[3] ha colmado ese vacío existente, si bien no ha sabido responder a todas las expectativas despertadas antes de su promulgación.

No obstante debe citarse entre sus aciertos el haber abordado la regulación de los denominados ***"datos sensibles"***.

El particular estudio de esta especial categoría de datos y su articulación en la legislación española, pretende ser el objeto de reflexión sobre el que versarán las siguientes consideraciones.

- 1 Cfr. **LOSANO, M. G.**: *Los proyectos de ley italianos sobre la protección de los datos personales*, en el vol. col.: *Problemas actuales de la documentación y la informática jurídica* (Actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986), ed. a cargo de A. E. Pérez Luño, Técnos & Fundación Cultural Enrique Luño Peña, Madrid, 1987, pág. 278.
- 2 Cfr. **TONIATTI, R.**: *Libertad Informática y Derecho a la Protección de los datos Personales: Principios de Legislación Comparada*, trad. cast. A. Saiz Arnaiz, en Revista Vasca de Administración Pública, 1991, Enero-Abril, nº 29, pág. 141.
- 3 Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Publicada en el BOE número 262, de 31 de octubre de 1992.

Conceptuación de los Datos Sensibles

Los datos personales, si por un lado pueden ser agrupados en una categoría homogénea, por otro, se prestan a ser reconsiderados de acuerdo con la diversa disciplina a la que está sometida su circulación. Una reconsideración respecto a la categoría general lo constituyen, precisamente, los datos sensibles. No existe un acuerdo unánime ni en la doctrina ni en el derecho comparado acerca de qué sean o qué deba entenderse por datos sensibles. Lo que sí parece existir es un acuerdo casi generalizado, en su abstracción, respecto a la necesidad de una regulación diferenciada respecto a ciertos datos personales cuyas peculiaridades exigen formas de tutela particulares.

Es precisamente en la determinación de esas peculiaridades donde surgen las discrepancias.

El Prof. **PEREZ LUÑO** considera como tales aquellos que tienen una inmediata incidencia en la privacidad o un riesgo para prácticas discriminatorias. También considera como tales aquellas informaciones que hacen referencia a convicciones personales, así como las referentes inmediatamente al resto de las libertades[4] .

TONIATTI por su parte establece una doble consideración respecto a la conceptualización de los datos sensibles:

- Criterio Formal: Aquellos datos que presentan algunos requisitos reforzados para que limiten su libre adquisición, circulación, etc...

- Criterio Material: Cualificados por su afectación a una esfera íntima subjetiva de particular delicadeza. Aquellos que más directamente se refieren ya a la esfera personal e íntima ya a la titularidad de los derechos fundamentales de libertad[5] .

MADRID CONESA, por último, estructura la consideración de los datos sensibles en torno a dos variables:

- 4 Cfr. **PEREZ LUÑO, A. E.**: *Libertad informática y leyes de protección de los datos personales*, en colab. con M. G. Losano y M. F. Guerrero Mateus, Centro de Estudios Constitucionales, Madrid, 1989, pág. 152; ID.: *Comentario Legislativo. La LORTAD y los derechos fundamentales*, en *Derechos y Libertades.* Revista del Instituto Bartolomé de las Casas, 1993, Febrero-Octubre, número 1, Universidad Carlos III de Madrid y Boletín Oficial del Estado, pág. 406.
- 5 Cfr. **TONIATTI, R.**: *Libertad Informática y Derecho a la protección de los Datos Personales: Principios de Legislación Comparada*, cit., pág. 155.

1. Aquellos cuyo tratamiento incorpora peligros de discriminación.

2. Aquellos que son irrelevantes desde el punto de vista de las relaciones externas de los ciudadanos; es decir, aquellos más directamente conectados con el ámbito más personal e íntimo [6].

Esta breve semblanza doctrinal nos ilustra respecto a lo que venimos señalando respecto a la conceptualización de los datos sensibles. Lo cierto es que, pese a todas las diferencias, existe un acuerdo respecto a una especial tutela, protección y garantías para estos datos.

Los datos sensibles, como cualesquiera otros datos, no pueden ser considerados estáticamente, sino en el proceso general de tratamiento automatizado del que constituyen su objeto, e incluso su fin. Surge aquí plantearse pues el carácter dinámico de su determinación.

Determinación de los Datos Sensibles: Su Dinamicidad

Dejando al margen la importancia que reviste la protección de ciertas categorías de datos que por su propia naturaleza pueden poner en peligro la intimidad de los ciudadanos, asistimos a un consenso casi generalizado respecto a la consideración de que no es la naturaleza de los datos la que atenta contra el derecho a la intimidad, sino el concreto contexto en el que se efectúa el tratamiento de dichos datos[7].

No es la clasificación abstracta de un dato como más o menos cercano al ámbito de las personas, ni la determinación de que por su naturaleza tiene carácter de secreto o no lo que determina su tutela, sino el ámbito concreto de su uso[8].

La tutela de las informaciones no puede ya quedar limitada a aquellas de cuya calidad así se exija, en una visión estática, sino que debe extenderse a la

- 6 Cfr. **MADRID CONESA, F.**: *Derecho a la Intimidad, Informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984, pág. 88.
- 7 Vid.sobre ello: *Propuesta de Directiva del Consejo, relativa a la protección de las personas en lo referente al tratamiento de datos personales*, Bruselas, 24 de septiembre de 1990, COM (90) 314 final- SYN 288. Asimismo art. 8 de 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 a la libre circulación de estos datos*, Bruselas, 15 de octubre de 1992, COM (92) 422 final- SYN 287.
- 8 Cfr. **DENNINGER, E.**: *El derecho a la autodeterminación informativa*, trad. cast. A. E. Pérez Luño, en el volumen a cargo de **A. E. Pérez Luño**, en el vol. col. *Problemas actuales de la documentación y la informática jurídica*, Técnos, Madrid, 1987, pág. 273.

dinámica de su uso o funcionalidad. Es evidente, como señala el **prof. Pérez Luño**, que cualquier información, en principio neutra e irrelevante, puede convertirse en sensible a tenor del uso que se haga de las mismas[9].

Existe la posibilidad, como venimos señalando, que datos a priori irrelevantes desde la consideración de la privacidad de las personas, sin embargo, en conexión con otros datos puedan servir para hacer completamente diáfana y transparente la personalidad de los ciudadanos.

Se aboga así por un sistema dinámico en la protección de los datos sensibles. La experiencia del Derecho Comparado, remisa a una amplia enumeración de la categoría de los datos sensibles, y su encorsetamiento en rígidas normas legales, nos dan una muestra de cuán inoperantes pueden ser las declaraciones grandilocuentes, paralelamente vacías de garantías.

Será el devenir de los tiempos, y el consecuente cambio en las estructuras sociales, el que determinará la inclusión o no de determinados datos en la categoría de "sensibles", y por lo tanto su acomodación a la realidad fáctica de su tratamiento.

Tiempo y espacio se revelan aquí como variables ineludibles de un verdadero y efectivo sistema de garantías.

No obstante, no todo será variabilidad, acomodación, sino que pese a las circunstancias cambiantes, siempre habrá un mínimo de "sensibilidad" que nos indicará el norte a seguir, y nos permitirá, alejándonos de la niebla, conocer ese mínimo irreductible que para el ser humano constituye su intimidad.

¿Numerus Clausus o Numerus Apertus?

El carácter dinámico que venimos propugnando en la determinación de los datos sensibles, nos lleva a plantearnos cuál debe ser la formula o método a través del cual deben positivizarse, y por lo tanto, determinarse su régimen específico y peculiar.

El decantamiento por una opción de numerus clausus o numerus apertus, dependerá, no tanto de la sensibilidad del legislador o de su mayor ampli-

■ 9 Cfr. **PEREZ LUÑO, A. E.**: *Comentario Legislativo: La LORTAD y los derechos fundamentales*, cit., pág. 413.

tud de miras, sino que lo realmente determinante será la concepción que se comparta acerca de la amplitud del bien jurídico protegido, bien limitado a la concepción individualista de la intimidad, o bien, además del anterior, al ejercicio efectivo del resto de las libertades. Por que como señala el profesor **Madrid Conesa**, el problema del derecho a la intimidad se resuelve, en última instancia, en un problema de libertad[10].

Por razones de seguridad jurídica es cierto que deberá procederse a la determinación legal de aquellos supuestos subsumibles bajo el ámbito de los datos sensibles. Ahora bien, será necesaria la utilización de cláusulas abiertas o generales, lo suficientemente precisas, en su vaguedad, como para determinar su ámbito de aplicación, pero, lo suficientemente amplias como para permitir la modelación en la conceptuación de los datos de acuerdo a las exigencias que demande el efectivo cumplimiento y garantía de los derechos de los ciudadanos.

Pasemos a ver algunos ejemplos de "determinación legislativa" de los datos sensibles.

Según la Convención Europea los datos sensibles (art. 6) son **"los datos de carácter personal que revelaren 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... y los referentes a las condenas criminales"**[11].

Las Comunidades Europeas enumeran como tales **"los datos que revelen el origen racial y étnico, la opinión política, las convicciones religiosas, filosóficas o morales, la afiliación sindical, así como las informaciones relacionadas con la salud y la vida sexual"**[12].

La Ley francesa (art. 31) incluye en esta categoría **"los datos nominativos que directa o indirectamente hagan constar los orígenes raciales o las opiniones políticas, filosóficas, religiosas o la afiliación sindical de las personas"**.

- 10 Cfr. **MADRID CONESA, F.**: *Derecho a la Intimidad, Informática y Estado de Derecho*, cit., pág. 45.
- 11 Vid. sobre ello: *Protección de datos. Convenio del Consejo de Europa de 1981*, Servicio Central de Publicaciones. Presidencia del Gobierno, Madrid, 1983, pp. 33-34.
- 12 Vid. sobre ello especialmente: Art. 8 de 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 a la libre circulación de estos datos*, cit.

En Gran Bretaña se incluyen (art. 2.3 de la *Data Protection Act*) **"los datos relativos al origen racial, a las opiniones políticas, religiosas o de otra naturaleza, a la salud física y mental, a la vida sexual y a las condenas penales"**.

Como se puede observar las categorías recogidas son casi idénticas, si exceptuamos las relativas a las condenas penales, cuya inclusión o no se debe a la diferente conceptuación con que los ordenamientos nacionales entienden la publicidad de las actuaciones penales y el régimen de los datos tratados o generados en tales actuaciones.

Conviene tener en consideración, que no será la enumeración de los datos la que determinará su efectivo régimen de garantías, sino la amplitud de supuestos que puedan subsumirse bajo su enumeración lineal. Es decir, se trata de un problema de interpretación acerca de qué debe entenderse bajo las dicciones legales de datos sensibles. Abordaremos este tema con más profundidad; baste ahora señalarlo.

Regulación de los Datos Sensibles en la Lortad.

Entre las muchas consideraciones hechas sobre la LORTAD cabe destacar positivamente el hecho de haber incluido en su articulado un apartado específico dedicado a la regulación de los datos sensibles, otorgándole una protección reforzada [13].

Para esta categoría de datos el principio general, es al contrario del existente para los datos ordinarios, el de la prohibición de recogida y tratamiento excepto en los casos previstos por la ley. Veámos si este presupuesto se cumple en nuestra norma patria. Para ello abordaremos su estudio desde distintos presupuestos.

A) Determinación de los datos sensibles.

La LORTAD procede en su art.7 a la determinación de los datos sensibles, bajo la denominación de datos especialmente protegidos. Acoge así el elemento de la protección, y de su diferente intensidad, como criterio delimitador de dicha categoría.

■ 13 Cfr. **PEREZ LUÑO, A. E.**: *Comentario Legislativo: La LORTAD y los derechos fundamentales*, cit., pág. 419.

Desde el punto de vista del afectado el elemento del consentimiento se revela como fundamental, como expresión máxima y global de su derecho a la autodeterminación informativa. La propia Exposición de Motivos así lo expresa: **"El principio de consentimiento... sus contornos, por otro lado, se refuerzan singularmente en los denominados "datos sensibles"..."**.

Pero no debe tratarse de un consentimiento simple, sino de un **"consentimiento informado"**, a fin de que el interesado pueda sopesar los riesgos y ventajas del tratamiento de sus datos sensibles y ejercer los derechos recogidos en la norma. Volveremos sobre este punto al tratar el régimen jurídico al que están sometidos.

B) Enumeración y Contenido.

El artículo 7 establece como datos sensibles **"los datos de carácter personal que revelen la ideología, religión y creencias, así como los referentes al origen racial, a la salud y a la vida sexual... los relativos a infracciones penales o administrativas"**.

Dos objeciones cabe hacer a esta enumeración legal:

1. Establece una parca regulación, consolidándose así un sistema de numerus clausus. No es esta afirmación contradictoria son la sostenida *supra* acerca de la necesidad de una generalidad en la dicción legal de los supuestos considerados como datos sensibles. El legislador español parece considerar los datos sensibles en función de una tutela estática, que presenta como referente ciertos preceptos constitucionales, cuya salvaguarda se propone llevar a efecto. Se consigue con ello sólo una solución parcial del problema.

Ha sido el Profesor **PEREZ LUÑO** el que con gran cierto ha puesto en evidencia la "parcialidad" que venimos señalando. Así se manifiesta el prof.. de la Hispalense: " *Hay que reprochar a la LORTAD el haber planteado la tipificación de las informaciones especialmente sensibles en función de la ideología, religión o creencias... 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 -hay que entender que también las realizadas a través de la informática- por razones de "nacimiento, raza, sexo, religión, opinión o cualquier otra circunstancia personal o social""* [14].

■ 14 Cfr. **PEREZ LUÑO, A. E.**: *Comentario Legislativo: La LORTAD y los derechos fundamentales*, cit., pág. 413.

2. Alusión a conceptos jurídicos ciertamente indeterminados, que no pueden considerarse como generales, en la postura que venimos defendiendo, sino ciertamente como ambiguos y que estoy seguro producirán en el momento de su alegación por algún ciudadano afectado, graves problemas de interpretación respecto al alcance de su contenido. Procederemos por ello a intentar dar una visión lo más completa posible acerca de qué supuestos son, a nuestro criterio, subsumibles bajo las expresiones legales contenidas en la LORTAD.

a) **Ideología**. Deberá incluir tanto las opiniones políticas, como las referentes a la afiliación sindical. Se englobarán las informaciones del interesado sobre sus actividades en el terreno político y sindical. Respecto a las informaciones referentes a la pertenencia a un sindicato nos adherimos a aquellos países que en sus legislaciones consideran que las informaciones referentes a la pertenencia a un sindicato llevan consigo riesgos para la intimidad personal.

Considerando la objeción que podría planteársenos respecto al requisito suplementario de la afiliación, en el ámbito sindical, recogido entre otras legislaciones por la Comunidad Europea, hacemos notar nuestra oposición a tal requisito suplementario. El conocimiento de las opiniones políticas tiene también su principal baluarte en la afiliación de los ciudadanos a los partidos políticos o en el desarrollo de actividades de apoyo, generalmente bajo la atenta mirada de los órganos rectores de los mismos. Así pues sólo quedan dos alternativas, o bien se prescinde en ambos casos del requisito de la afiliación como elemento delimitador de la adscripción a una determinada opción política o sindical, o bien, se exige en ambos casos, con el riesgo evidente de limitación del ámbito material protegido [15].

b) **Religión y Creencias**. Se considerarán como tales las creencias religiosas, convicciones filosóficas y morales, incluida la falta de creencias religiosas, así como las informaciones relativas a las actividades del interesado en el terreno religioso o filosófico, y las actividades o actitudes que se deriven de tales creencias o convicciones. Las creencias no religiosas o no filosóficas también deben constituir datos especiales.

c) **Origen racial**. Comprende los datos o informaciones relativos a la pertenencia a una etnia, pueblo o nación, al margen de su adscripción a un determinado Estado. Deberá incluirse asimismo la información sobre el color de la piel.

■ 15 Vid. sobre ello: *Protección de datos. Convenio del Consejo de Europa*, cit., pág. 33. Asimismo *Propuesta modificada de Directiva* ..., cit., pág. 18.

d) **Salud**. Los datos personales relativos a la salud pueden catalogarse, como hace **Toniatti**, de supersensibles[16]. Conciernen a un ámbito merecedor de información reforzada hasta el punto de excluir normalmente el acceso directo de los individuos a los propios datos personales[17]. Abarca las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. Pueden tratarse de datos referentes a un individuo de buena salud, enfermo o fallecido. Estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas. Deben hacerse, no obstante, dos consideraciones respecto a este tipo de datos:

1. Habrá que tener especial cuidado respecto a los datos referentes a la salud mental en el futuro, pues se corre el riesgo de hacer ingresar a los afectados en una especie de "censos negros", con el paralelo peligro para el ejercicio de sus derechos. Se puede así proceder al tratamiento de estos datos sensibles basándose en meras sospechas que no presenten ninguna constatación fáctica. Serán las verdaderas necesidades del tratamiento médico y la evolución de la enfermedad, junto a unas razonables previsiones de futuro, las que deben determinar la inclusión de estos datos.

2. Respecto a las referencias al alcohol y a las drogas, deberán establecerse límites flexibles, atemperados a los efectos particulares sobre el individuo concreto. Máxime cuando no está claro ni para el Derecho Penal, ni para la Ciencia Toxicológica, dónde están los límites entre el consumo, uso y abuso de drogas o alcohol. La estricta referencia al término drogas engloba otras sustancias perjudiciales para la salud, tales como los estupefacientes y los psicotrópicos.

e) **Vida Sexual**. Es este un término ciertamente relativo y estrictamente personal. Como señala el prof. **López Ibor** la conducta sexual relativa al objetivo que la motiva puede ser influida por los actos positivos o negativos referentes a la finalidad de lo sexual en sí. Por lo tanto varía notablemente según los individuos, desplazándose desde el mismo acto sexual a sus elementos y derivados más o menos remotos[18].

- 16 Cfr. **TONIATTI, R.**: *Libertad Informática y Derecho a la Protección de los Datos Personales: Principios de Legislación Comparada*, cit., pp. 158-ss.
- 17 Vid. sobre ello y en el ámbito de la política comunitaria de protección de los datos personales: *Propuesta modificada de Directiva...*, cit., especialmente su artículo 13 donde a propósito del reconocimiento del derecho de acceso de los interesados, establece en su apart. 1.2: *Los Estados Miembros podrán prever que el derecho de acceso a los datos de carácter médico únicamente pueda ejercerse por medio de un médico.* Se pretende con ello, como ha señalado la propia Comisión en esta su propuesta, proteger al interesado de cualquier conmoción que pudiera tener graves repercusiones psicológicas, que puedan producir, en casos extremos, incluso el suicidio.
  Sobre la política desarrollada en Francia y Gran Bretaña respecto al acceso a los datos médicos, especialmente de afectados por el SIDA, vid.: **TONIATTI, R.**: *Libertad informática y Derecho a la Protección de los Datos Personales: Principios de Legislación Comparada*, cit., pp. 159-ss.
- 18 Cfr.: *El Libro de la Vida Sexual*, dirig. por J.J. López Ibor, Danae, Madrid, 1968, pág. 410.

Deberán incluirse por lo tanto todos los datos relativos a la actividad sexual de los ciudadanos, así como la ausencia de dicha actividad, y las consecuencias que de ellas se derivan.

Se considerarán también como tales los datos de "referencia indirecta", es decir aquellos de los que puedan extraerse ciertos datos indiciarios de su conducta sexual, tales como suscripción a revistas de contenido erótico, anuncios de contactos, pertenencia a ciertos colectivos de defensa de homosexuales o/y lesbianas, etc...

e) **Infracciones penales o administrativas.** Debe partirse de la incorrecta denominación empleada por el legislador español para hacer referencia a estos datos. Debería haber empleado más bien el de **condenas**, por cuanto que son las sentencias en las que éstas se establecen las que incorporan una serie de datos que pueden menoscabar gravemente la intimidad de los ciudadanos. Si a ello unimos la conservación de datos referentes al cumplimiento de las mismas, una vez que dichas condenas han sido ya cumplidas o se han extinguido, el potencial lesivo es enorme.

Las mismas consideraciones caben, *mutatis mutandi*, respecto del empleo del término infracciones administrativas.

Por tales infracciones deberán entenderse las sanciones fundadas en una norma penal o administrativa e impuestas en el marco de un procedimiento penal o sancionador-administrativo.

C) Régimen jurídico.

Como señalamos anteriormente la regulación de los datos sensibles en la LORTAD, se configura en torno al principio del consentimiento. El consentimiento de la persona concernida acerca del tratamiento de sus datos sensibles se constituye como elemento fundamental articulador del sistema de garantías.

Será el consentimiento, y sus diferentes manifestaciones, el que determinará la posibilidad de tratamiento automatizado de estos datos. Se constituye así un sistema de "regulación en cascada", que desde la elaboración de un principio general desemboca en una posibilidad casi absoluta de tratamiento, si bien sólo circunscrita a los ficheros de carácter público.

Veámos como queda configurado este esquema regulador.

1. Principio General. Prohibición de recogida y tratamiento excepto con el consentimiento del afectado, o en los casos previstos por la ley. El consentimiento, como ya señalamos, debe ser informado, para permitir así al afectado evaluar las ventajas e inconvenientes que se derivan de dicho tratamiento. Este consentimiento informado se recoge en la LORTAD en el apartado 2, punto 1, artículo 7 cuando señala: *"Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo"*. No obstante se echa en falta en la dicción legal la referencia al carácter de libre del consentimiento, que no por obvio, deja de ser menos necesario. Coadyuva a este principio general, la prohibición de crear ficheros con la finalidad exclusiva de almacenar datos sensibles.

2. Consentimiento de Primer Grado. Los datos de carácter personal que revelen la **ideología, religión y creencias**, sólo podrán ser objeto de tratamiento con *consentimiento expreso y por escrito*. Estos requisitos evidencian, como señala la propia Exposición de Motivos, el carácter reforzado de la protección de estos datos, adquiriendo así el carácter de "supersensibles".

3. Consentimiento de Segundo Grado. Sólo con el *consentimiento expreso* del afectado podrán tratarse datos referentes al **origen racial, a la salud y a la vida sexual**.

Aquí ya no es necesario la plasmación por escrito del consentimiento para proceder al tratamiento. Sólo se exige que sea expreso, y por lo tanto podrá manifestarse de forma oral. Ello conlleva unos evidentes problemas probatorios para el afectado, no sólo en la determinación de si otorgó o no el consentimiento, sino también respecto al alcance del mismo.

Pero lo verdaderamente sorprendente, cosa que no se acierta a comprender, es la diferenciación entre grupos de datos sensibles. Se crean así datos de *primera y de segunda clase*, sin una razón que lo justifique. La deficiente referencia a un precepto constitucional, como base de la determinación de los datos sensibles, puede ser la raíz de tamaño error. El legislador olvida que la intimidad de los ciudadanos no conoce de parcelaciones cuando al tratamiento de los datos sensibles se refiere.

4. Habilitación legal por razones de interés general. Las críticas apuntadas anteriormente se acentúan ante esta posibilidad, que presenta como único anclaje con la legalidad la abstracta e indeterminada referencia al interés general. Nada hace el legislador para colmar nuestras dudas. Sólo hay una cosa cierta, por esta vía se abre una puerta para el tratamiento de datos referentes al **origen racial, a la salud y a la vida sexual**.

Será preciso determinar en este instante qué se entiende por interés general.

Siguiendo lo señalado por la Comisión de las Comunidades Europeas, pueden considerarse englobadas en tal denominación genérica todas aquellas medidas necesarias para la salvaguarda de los valores fundamentales de una sociedad democrática[19]. En idénticos términos se expresa el Consejo de Europa[20].

Pero la concurrencia de dicho interés general deberá hacerse constar mediante una Ley. Nada dice el texto acerca del rango normativo de esta norma habilitante. Sólo la Exposición de Motivos hace referencia a la misma, añadiéndole que la habilitación legal habrá de ser expresa.

Ante esta falta de previsión legal conviene señalar que en dicha disposición legal deberán precisarse los datos que pueden ser tratados, las personas destinatarias de los mismos, la cualificación del responsable del tratamiento, las personas autorizadas a acceder a ellos, así como las garantías apropiadas contra los usos abusivos y los accesos no autorizados.

Sólo con estas menciones de la norma habilitante podrán salvarse las garantías que para los derechos de los ciudadanos establece la propia LORTAD.

5. Libertad de tratamiento, aunque sólo referido a los ficheros automatizados de las Administraciones Públicas.

Los datos de carácter personal referentes a la **comisión de infracciones penales o administrativas** sólo podrán ser incluidos en ficheros automatizados de las Administraciones Públicas. Sirvan en este punto lo señalado *supra* acerca de qué debe entenderse por tales infracciones, y las consecuencias que de ello se derivan.

D) Excepciones a la prohibición de tratamiento de datos sensibles: Ficheros de las Fuerzas y Cuerpos de Seguridad.

El estudio del régimen jurídico de los datos sensibles en nuestro ordenamiento, quedaría incompleto si no recogiéramos también las excepciones que

■ 19 Cfr.: *Propuesta modificada de Directiva...*, cit., pág. 26.
■ 20 Cfr.: *Protección de datos. Convenio del Consejo de Europa de 1981*, cit., pág. 36.

establece la misma ley. Es precisamente en éstas donde hay que mirar para ver cuál es el efectivo sistema de protección y de garantías otorgado a los ciudadanos. Declarados rimbombantemente una serie de derechos, es habitual su derogación posterior de manera soterrada o encubierta, amparándose en ineludibles deberes del Estado, dando una imagen garantísta al ciudadano, cuando realmente lo que se está configurando es un verdadero asalto a sus derechos y libertades.

La LORTAD recoge, en esta línea, la posibilidad de tratamiento automatizado de datos sensibles **en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta (art. 20.3)**.

De nuevo el legislador español acude a conceptos jurídicos indeterminados, que lejos de aportar flexibilidad en su articulación, lo que hacen es atraer negros nubarrones sobre cuál es el verdadero alcance de esta excepción. Se trata, como vemos, de una regulación fundada en un criterio restrictivo sobre la subsistencia de un derecho individual merecedor de protección que deja paso al prevalente interés nacional[21].

La circunstancia "objetiva" que determina la posibilidad de dicho tratamiento son los fines de una investigación concreta. Este término debe incluirse dentro del marco más amplio de la **"represión de los delitos"**, y que comprendería tanto la investigación de los delitos como su persecución. Esta posibilidad, que pudiera parecer lógica como medio de salvaguarda de la **seguridad pública**[22], sin embargo adolece de tal carácter ante la total desarticulación del sistema de garantías de los ciudadanos.

Esta permisividad de la legislación española choca con los estrictos límites que en el Derecho Comunitario se pretenden establecer respecto a estos tratamientos, y que se concretan en la imposibilidad de las Fuerzas y Cuerpos de Seguridad de proceder al tratamiento de dichos datos.

■ 21 Cfr. **TONIATTI, R.**: *Libertad Informática y Derecho a la protección de los Datos Personales: Principios de Legislación Comparada*, cit., pág. 157.

■ 22 En torno a la delimitación del concepto de seguridad pública, el Consejo de Europa, en la Memoria Explicativa, número 56, del Convenio 108 para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, establece que **"la noción de seguridad del Estado deberá entenderse en el sentido tradicional de protección de la soberanía nacional contra amenazas internas o externas, incluida la protección de las relaciones internacionales del Estado"**, vid. sobre ello: *Protección de datos. Convenio del Consejo de Europa*, cit., pág. 36.
Por su parte las Comunidades Europeas consideran como tal **"todas las actuaciones policiales de los órganos del Estado, incluida la prevención del crimen"**, vid. sobre ello: *Propuesta modificada de Directiva...*, cit., pág. 25.

En la legislación española, por contra, se deja a los propios responsables del tratamiento la determinación "unilateral", de cuándo los datos deberán ser utilizados, así como la amplitud material y temporal de dicha utilización. Difícilmente conocerá el afectado que se está procediendo a una utilización de sus datos sensibles por parte de las Fuerzas y Cuerpos de Seguridad. Además se exime a éstos de la concesión a los afectados de los derechos de acceso, rectificación y control. Esto parece ser, en su sin razón, lo más coherente. Si un ciudadano desconoce que sus datos sensibles están siendo objeto de tratamiento automatizado por parte de las Fuerzas y Cuerpos de Seguridad, difícilmente tendrá la "necesidad", por ese desconocimiento, de ejercitar los restantes derechos.

El problema no está sólo en la derogación de los derechos de los ciudadanos, sino fundamentalmente en la consolidación de una potestad ciertamente arbitraria.

Ultimas consideraciones. A modo de conclusión.

La protección de los datos personales sensibles dista mucho de ser satisfactoria en la forma establecida por nuestra legislación.

Su indeterminación, sus imprecisiones y sus alarmantes excepciones no hacen más que ahondar en esa desprotección que para el ciudadano, y en la esfera de sus datos personales, parece consolidarse.

Es aquí donde una vez más se revela imprescindible una conciencia social informada, crítica, que sea capaz de rebelarse contra las vulneraciones de sus derechos, y de exigir el efectivo y total cumplimiento de los mismos.

Pero esta no es una tarea que competa exclusivamente a los ciudadanos. El Estado como garante de los derechos y libertades públicas deberá proceder a las adaptaciones necesarias para que la salvaguarda de aquéllos responda a la exigencias de un Estado Social y Democrático de Derecho. Hasta que ello sea posible, continuará siendo necesario mantener una postura crítica.

La Seguridad y la Confidencialidad de la Información y la LORTAD

MIGUEL ANGEL RAMOS

Doctor en Informática. CISA. Vicepresidente de la Organización de Auditoría Informática y del Capítulo Español de la EDP Auditors Association, consultor en seguridad y auditor informático.

1. Introducción

Cada día la información tiene más importancia para las entidades, que basan en mayor medida su gestión en la disponibilidad de una información correcta, completa y a tiempo, por lo que es creciente la importancia de su seguridad y su confidencialidad.

La LORTAD se refiere a la confidencialidad de los datos de carácter personal, pero puede ser una excelente oportunidad para mentalizar a los "propietarios" de la información y directivos en general, ya que muchas de las medidas y controles pueden servir tanto para garantizar la confidencialidad como la seguridad en general, y lógicamente no sólo de los datos de carácter personal sino de todos ellos.

Los objetivos de la seguridad abarcan: las personas (y funciones que desempeñan, con la debida segregación), las propias instalaciones, los equipos y comunicaciones, los programas y, muy especialmente, los datos.

La seguridad y confidencialidad debe tratarse a un nivel corporativo, a través del oportuno Comité, que apruebe políticas y planes al respecto y aporte los medios necesarios para poder abordar con rigor la protección de la información y realizar un seguimiento en el tiempo sin relajaciones.

El primer paso es conocer qué riesgos existen para poder decidir cómo eliminarlos o al menos disminuir su impacto y/o la probabilidad de que se produzcan.

Las protecciones han de ser físicas y lógicas (entre éstas últimas están los paquetes de control de accesos), y existir una separación de entornos y una segregación de funciones, además de una clasificación de la información; y deben existir los medios para garantizar su eficiencia: asignación de responsables de los ficheros, administración de la seguridad, auditoría informática interna (y posible contratación de la externa).

A veces relacionamos seguridad informática con desastres, pero existen también pérdidas, errores, omisiones o filtraciones de información, de menor impacto pero mucha mayor probabilidad.

Por otra parte, la ausencia generalizada de noticias respecto a casos habidos en España no quiere decir que éstos no se produzcan, sino que se mantienen más en secreto que en otros países, para preservar la buena imagen de las entidades, por lo que no salen de círculos reducidos, y no pueden comentarse en conferencias o seminarios.

2. Protagonistas

La seguridad y confidencialidad de los datos automatizados (contenidos en cualquier soporte legible por ordenadores) no debe considerarse un tema puramente técnico. Los "propietarios" de la información y los directivos en general no pueden "abdicar" en los informáticos escudándose en su ignorancia, y deben aportar las líneas maestras (sin entrar en tecnicismos) y tener la garantía de que se están cumpliendo sus requerimientos, por ejemplo en cuanto a quién puede acceder a qué, cuánto tiempo se está guardando determinada información o qué controles existen para garantizar la integridad de los datos más críticos (nos referimos a datos críticos y no "sensibles" como recoge la propia LORTAD, que es una expresión muy usada, y que tal vez deriva de forma indirecta del inglés: "sensitive data").

Además, existirán los administradores de datos y de bases de datos, y los responsables de ficheros, figura recogida en la LORTAD y que expertos más autorizados han tratado en estas Jornadas en ponencias específicas.

Otros protagonistas (indirectos) son los usuarios, a quienes los propietarios habrán de autorizar a qué pueden acceder y cuándo.

Los informáticos son meros administradores de la información que procesan, aunque deben contribuir a garantizar a propietarios y usuarios que existen las medidas adecuadas.

Puede existir una función específica de Administración de la Seguridad (física y/o lógica), como interfaz entre propietarios, usuarios e informáticos.

Además, es deseable que exista la función de auditoría informática interna (y/o contratar auditoría informática externa, que son compatibles y complementarias), para que revisen si existen los controles adecuados, determinen cuáles pueden ser los riesgos y recomienden las medidas a implantar o reforzar. Dichos auditores han de contar con la preparación adecuada, además de la suficiente objetividad e independencia y, lógicamente, no pueden depender de la función de administración de seguridad ni viceversa.

En cuanto a controles, recordemos que se dice que han de ser: completos a la vez que simples, fiables, revisables, adecuados y rentables; y en cuanto a su coste, hay que considerar el de implantación y el de mantenimiento, frente al coste-riesgo de su no implantación. Los controles en general suelen dividirse en:

- controles preventivos: los que contribuyen a evitar que se produzca el hecho: el incendio, el acceso...

- controles detectivos: los que, una vez que se ha producido, ayudan a conocer el hecho, como la revisión de listados de ordenador con los documentos base como órdenes de clientes, para detectar errores y fraudes,

- controles correctivos: los que contribuyen a restaurar la situación de normalidad, como la recuperación de un fichero dañado a partir de copias de procesos anteriores.

3. La Lortad

La Ley, en su artículo 9 especifica:

1. El responsable del fichero deberá 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 automatizados 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 automatizados y las personas que intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de esta Ley.

El Estatuto de la Agencia de Protección de Datos (Real Decreto 428/93, BOE 4-5-93), en su artículo 28 determina sus funciones inspectoras (se resume el contenido):

- Examinar los soportes de información que contengan los datos personales
- examinar los equipos físicos
- requerir el pase de programas y examinar la documentación y algoritmos de los procesos
- examinar los sistemas de transmisión y acceso a los datos
- realizar auditorías de los sistemas informáticos.

Se trata de una de las pocas referencias que existen a la Auditoría Informática, actividad que no tiene reconocimiento oficial y no está regulada por ahora.

4. Areas

Hay muchos aspectos a considerar en relación con la seguridad y confidencialidad de la información, y algunos tienen una relación muy estrecha.

Entre ellos están:

*La existencia de planes, presupuestos y definición de niveles de responsabilidad. La seguridad y la confidencialidad deben ser una preocupación prioritaria de la Alta Dirección de la entidad, además de serlo de los propietarios de la información de cada área y de los usuarios y administradores.

La realidad es que si ocurre algo siempre se buscan "culpables", pero el enfoque debe ser preventivo, no a hechos consumados.

Es aconsejable que exista un Comité que se ocupe de la seguridad y confidencialidad. Si la entidad es importante puede tener ese cometido en exclusiva; si no, puede ser el propio Comité de Sistemas de Información (o de Informática) o el Comité de Dirección el que trate sobre estos temas en sus reuniones.

Uno de las primeras acciones deberá ser la definición de políticas y la elaboración de planes (plan de seguridad y de confidencialidad, plan de contingencia o de continuidad) y la aportación de los medios necesarios.

La mentalización de todo el personal también es un punto que no se debe pasar por alto, así como la asignación de medios, no sólo económicos sino "tiempo" a quienes tienen que dedicarse a ello, a menudo como otra tarea más a añadir a una larga lista. La colaboración externa puede aportar objetividad, experiencia y ritmo a este tipo de proyectos.

*Administración de la seguridad. Esta función puede tener, entre otros, los cometidos siguientes, que debieran definirse por escrito:

-Proponer políticas y estándares sobre seguridad y confidencialidad de la información,

-"Administrar" la seguridad: formación e información, así como establecimiento y revisión de controles (si existe auditoría informática interna, será ésta la que realice las revisiones),

En cuanto a la seguridad lógica (en contraposición a la física), participación en la selección e implantación de paquetes de seguridad, así como de la

propia seguridad de los diferentes productos y aplicaciones y el correspondiente seguimiento. Mantenimiento de usuarios (altas, bajas y variaciones de perfiles) y revisión de los informes que proporcione el paquete.

*La ubicación del centro de procesos y de los ordenadores: la ubicación ha de ser idónea para garantizar la seguridad y que sólo acceden las personas autorizadas. Si se trata de equipos departamentales o personales aislados igualmente deben estar protegidos para evitar el robo.

Dicho robo puede referirse al propio equipo, que a veces no sería tan importante como de la información que contuviera si no está debidamente respaldada en otro lugar, o si el conocimiento por terceros puede suponer pérdida de competitividad o de imagen.

Las instalaciones, por tanto, han de tener los mecanismos y controles necesarios: sensores, infrarrojos, blindajes, cámaras de televisión (que pueden visualizar vigilantes y que pueden ponerse en funcionamiento cuando se produzca movimiento), exigencia de marcar contraseñas para que se abran las puertas o para otros accesos... y todo ello según la criticidad de la información y la existencia de otros controles.

Otra medida complementaria es la contratación de seguros, más bien a los efectos de la recuperación económica, lo que no evita que se haya producido una pérdida irrecuperable de información y con las consecuencias indirectas que puede suponer.

*Hemos hablado de seguridad lógica, es decir de los accesos a través de terminales, locales o remotos. Es necesario decidir (los propietarios han de determinarlo o al menos las reglas generales) quién puede acceder a qué, para qué (lectura, borrado, variación...) y cuándo. También deben determinarse las pistas necesarias que han de quedar para poder hacer revisiones por otras personas.

A propósito de los accesos es importante la asignación de contraseñas, que son uno de los medios más comunes (y económicos) de identificarse ante un sistema, sobre todo ante una aplicación o un paquete de control de accesos, que dé la posibilidad de acceder o no a determinados recursos.

La identificación ante un sistema puede ser:

-Por algo "que se es": apariencia / foto del individuo. En algunos casos se está usando la biométrica, en base a los caracteres diferenciadores de los individuos, como retina o huella dactilar,

-por algo que se realiza: la firma, por ejemplo; existen sistemas automáticos de reconocimiento de firmas, con porcentajes muy pequeños de error,

-por algo que se tiene: por ejemplo, una tarjeta; cada vez se utilizan más las tarjetas "inteligentes" (el adjetivo puede no ser el más adecuado aunque sea la traducción más usada de "smart cards"), que tienen grabada información y que pueden contener la fotografía del individuo y/o la firma digitalizadas,

-por algo que se sabe, como la propia contraseña. El problema radica en poder garantizar que la persona que está marcando una contraseña es aquella a la que se asignó y no un "suplantador", que ha conocido la contraseña de forma casual o se la han cedido. De ahí la utilidad de combinar las contraseñas con biométrica u otros sistemas.

A propósito de las contraseñas, está demostrado que cada vez es menor el número de casos en que alguien "entra" en un sistema a base de intentos hasta acertar la contraseña, ya que se limita el número de ellos.

Así, por ejemplo, si después de tres intentos fallidos no ha sido capaz de acceder al sistema, el usuario como tal queda inactivo, y el administrador del sistema lo reactivará después de averiguar qué está pasando: es posible que el verdadero usuario haya vuelto de vacaciones y haya olvidado su contraseña, pero también puede ocurrir que alguien no autorizado, suplantando al verdadero usuario, esté intentando acceder. Si sabe que al tercer intento el sistema bloqueará ese código de usuario hará dos intentos cada día, pero esto también puede registrarlo un paquete de control de accesos y pasar esta información a un administrador para que investigue.

Las contraseñas, que tanta relación tienen con la seguridad de la mayoría de los sistemas que existen hoy en día, deben ser fáciles de recordar por su "propietario", para evitar tener que escribirla (como ocurre a veces con las que asignan de forma aleatoria los sistemas). Así, costará recordar una contraseña como "L3*2P7".

Si la asigna su "propietario" y no el sistema, debe ser difícil de imaginar por los demás, evitando datos obvios como el número de empleado, el de la matrícula de su coche o el nombre del cónyuge.

Deben tener una longitud mínima y poder combinar cifras y letras. Con una longitud de seis caracteres, y si contamos las letras, las cifras del 0 al 9 y algunos símbolos especiales, tenemos 42^6 posibilidades.

Algunos sistemas sofisticados (por ejemplo el paquete RACF de IBM), permiten forzar a los usuarios a que no reasignen ninguna de las "n" contraseñas anteriores. El número "n" lo asigna el administrador.

La caducidad es otro de los puntos importantes, ya que cuanto mayor sea la vida de una contraseña más vulnerable será: cada entidad debe fijar criterios al respecto, y un periodo de un mes puede constituir un plazo razonable. Existen sistemas más críticos con contraseñas de un día de vida (un turno de trabajo, por ejemplo) e incluso contraseñas de un solo uso.

Las contraseñas deben estar criptografiadas internamente en los ficheros y no aparecer "en claro" en las pantallas ni en los listados.

Las entidades deben recordar a sus empleados mediante procedimientos la prohibición de ceder la contraseña, ya que se pierde la "imputabilidad"; no será fácil atribuir una operación o transacción si varias personas en un departamento comparten una misma contraseña.

Por tanto, los sistemas deben obligar a los usuarios a identificarse y éstos "salirse" del sistema para obligar a otros a identificarse antes de comenzar su consulta o marcaje de datos.

Con demasiada frecuencia las contraseñas se ceden temporalmente o se teclean a la vista de otros (si se averiguan algunos de sus caracteres, o al menos que se trata, por ejemplo, de la parte izquierda superior del teclado, el número posible de combinaciones disminuye); debe existir la mentalización adecuada en cada entidad sobre el uso y custodia de las contraseñas.

También contribuye a incrementar la seguridad el hecho de que los terminales queden inactivos después de varios minutos sin uso, para evitar que otras personas no autorizadas conozcan lo que se muestra en la pantalla o incluso accedan a las aplicaciones y datos a que tienen acceso los usuarios primarios por abandono momentáneo de éstos.

*El desarrollo de aplicaciones: los desarrolladores, tanto internos como externos contratados, no tienen por qué conocer los datos "reales" críticos: contables, de empleados, de clientes... y de ahí que deba existir una separación de entornos suficiente, tanto física como lógica.

Y en los casos en que pueda ser necesario hacer pruebas con datos reales confidenciales, pueden existir programas que "camuflen" dichos datos, susti-

tuyendo los campos críticos para que, sin perder sus características, no contengan domicilios, nombres o saldos reales.

Por otra parte, en el momento del desarrollo pueden incorporarse algunos controles que ayuden a garantizar la integridad de la información y que avisen de situaciones anómalas que se detecten, por mal funcionamiento de programas o por accesos indebidos.

*Los datos: además de la clasificación (de uso restringido, departamental, confidencial...) debe existir segregación de funciones en cuanto a las diferentes fases del ciclo de vida de los datos y revisiones posteriores para confirmar que son veraces y están respaldados por, según los casos, órdenes de clientes, autorizaciones de pago...

También debe vigilarse que los datos en soportes magnéticos o en papel estén protegidos, incluso cuando ya no son necesarios (porque pueden seguir siendo confidenciales); así, el papel habrá de ser destruido, en vez de tirarlo o venderlo, y los soportes magnéticos deben borrarse expresamente mediante varias pasadas de grabación o, mejor aún, desmagnetizarse con dispositivos al efecto, ya que de lo contrario puede quedar información no "machacada" accesible por rutinas especiales o incluso leerse la que ha estado grabada previamente "debajo" con dispositivos muy sofisticados.

Tanto en los datos almacenados como en los transmitidos por línea puede usarse la criptografía, para que los que puedan acceder a los datos no estando autorizados para ello, encuentren dificultades y les resulte virtualmente imposible conocer la información; aunque en la práctica dependerá de la vulnerabilidad de los métodos empleados y de los medios con que cuenten los criptoanalistas.

En instalaciones más complejas puede convenir instalar arcos detectores de soportes magnéticos, que avisarían de los que tanto empleados o visitantes puedan intentar sacar de la instalación.

En cuanto al transporte de soportes magnéticos, puede realizarse por empresas especializadas o, en entornos menos sofisticados, en dispositivos cerrados y cuya llave y/o clave no esté en poder de las personas que realizan el transporte o esté suficientemente protegida (por ejemplo en sobre lacrado).

5. Riesgos

En definitiva, deben establecerse los procedimientos y controles necesarios para poder garantizar que cada usuario sólo accede:

-a lo que esté autorizado (instalaciones, programas, bases de datos, ficheros, campos...)

-para lo que esté autorizado: lectura, variación, borrado...

-cuando esté autorizado, en cuanto a fechas y horas.

Para prever situaciones de emergencia, es preferible no abrir excesivamente los perfiles de acceso, sino que existan usuarios con posibilidades excepcionales, incluso no asignados de forma permanente sino que cuando sean necesarios se entreguen en sobre cerrado a quienes lo necesiten, dejando constancia de ello, por ejemplo a través de un vigilante de seguridad física que custodiara el sobre, para que se pueda verificar después el uso de la contraseña especial y si su uso estaba justificado.

Esto puede ser útil en situaciones que pueden presentarse fuera de los horarios normales de trabajo, para recuperación de información o variaciones de programas o tablas por emergencias, y salir de situaciones de bloqueo que impidan la continuación de los procesos.

Los riesgos principales son:

-los accesos no autorizados, por las causas ya comentadas,

-la destrucción o "corrupción" de datos: por ejemplo las tablas de devengos, los porcentajes de liquidación, los domicilios, borrado de "pistas" en ficheros históricos...

-la manipulación de programas, que puede traducirse en destrucción o variación de datos, incluso pasado un tiempo alcanzada una circunstancia (lo que se denomina "bomba lógica", en contraposición a física), y que puede manifestarse, por ejemplo, llegada una fecha o cuando un campo alcance un valor determinado, por lo que puede resultar una lotería macabra; puede manifestarse cuando el autor ya no está en la entidad, que es a veces la finalidad: producir el daño pero no sufrir las consecuencias,

-En ocasiones lo que se persigue es el propio beneficio, por ejemplo la copia de programas o de datos, en el primer caso para evitar gastos y en el

segundo para conocerlos y así saber la situación de la entidad o los datos de sus clientes, por ejemplo, o bien para cederlos a terceros a cambio de un beneficio económico.

Ante cualquier incidencia es necesario investigar las consecuencias que ha habido para tratar de solucionarlas y averiguar qué ha fallado: si los controles no son rígidos, si ha habido encubridores, si los procedimientos son adecuados pero no se han cumplido...

6. Conclusiones

Es evidente que existe una necesidad de garantizar la seguridad y confidencialidad de la información, que será mayor según lo crítica que ésta sea en cada entidad, lo que vendrá determinado en buena medida por el sector.

La LORTAD es una buena ocasión para reforzar los mecanismos de protección que puedan garantizar la seguridad y confidencialidad de la información hasta unos niveles prefijados, ya que muchos de esos mecanismos son comunes.

Las consecuencias del incumplimiento de la LORTAD pueden traducirse en multas de hasta cien millones de pesetas, pero, además, hay que considerar otras posibles pérdidas: en cuanto a la falta de confidencialidad la pérdida de imagen y hasta de clientes; en lo que se refiere a la seguridad como tal, en los casos más graves, hasta la posible discontinuidad del funcionamiento de la entidad.

No obstante, la inversión en seguridad (y debemos hablar de inversión y no de gasto) es baja en España, salvo en algunas entidades aisladas, sobre todo del sector financiero o entornos militares y algunas multinacionales extranjeras.

Algunas de las medidas no son caras y es por ellas por las que debemos empezar; así, el conocer los riesgos y el implantar controles simples y procedimientos suelen constituir medidas de coste bajo y rentabilidad alta.

Podemos preguntarnos: ¿es mayor el coste de las medidas para garantizar la seguridad y confidencialidad o que no existan?. Antes de contestar, debemos considerar las pérdidas indirectas que podemos sufrir, así como que la falta de seguridad puede suponer como decíamos, ante una incidencia informática importante, la pérdida de toda la información vital y posiblemente el fin de la actividad de la entidad.

Bibliografía

- Auerbach: Data Security Manual

- Datapro: Computer Security (tres tomos). 1991

- Del Peso Navarro, Emilio. Prevención vs fraude: la Auditoría Informática. Actas del III Congreso Iberoamericano de Informática y Derecho. Mérida, 1992.

- Pfleeger, Charles P. Security in Computing. Prentice-Hall, 1989

- Ramos, Miguel Angel. Tesis Doctoral "Contribución a la mejora de las técnicas de auditoría informática mediante la aplicación de métodos y herramientas de ingeniería del conocimiento". F. de I. de la U.P.M.

- Ramos, M.A. La importancia de la seguridad informática. Computerwold, marzo 1990.

- Ramos, M.A. La Auditoría de la Seguridad. CHIP, marzo 1992.

- Ramos, M.A. Ponencias en Securmática en 1991 y 1992 y material de seminarios propios.

- S. Rao Vallabhanenei. Auditing Computer Security. John Willey & Sons, 1989.

EL SECRETO ESTADISTICO: Contenido Jurídico

JORDI BACARIA MARTRUS
Generalitat de Cataluña.
Asistencia Técnica Estadística.
Departamento de Economía y Finanzas.
Instituto de Estadística de Cataluña.

1. Definición. Características y Límites del Secreto Estadístico.

El secreto estadístico es una figura de derecho administrativo especial que consiste en la obligación de preservar el anonimato de los datos individuales, obtenidos en la realización de las actividades estadísticas para los servicios estadísticos de las administraciones públicas, a fin de proteger el bien jurídico que constituye la intimidad de las personas, entendido en el sentido más amplio de aquello que hoy podemos denominar privacidad.

El secreto estadístico tiene como fundamento jurídico el derecho subjetivo a la intimidad, considerado como una parcela de los bienes de la personalidad.

El secreto estadístico constituye un deber jurídico por mandato imperativo de la ley que obliga a todo el personal estadístico y también a las personas físicas y jurídicas que tengan conocimiento de la información estadística indi-

vidualizada y a los órganos de la Administración titulares de la función pública estadística, a no difundir ni directa ni indirectamente datos individuales o individualizados de los suministradores de la información.

El secreto estadístico protege al suministrador de datos, tanto si se trata de una persona física como jurídica, de cualquier revelación que conduzca a la identificación de datos personales.

El ordenamiento jurídico otorga, por medio de la figura del secreto estadístico, una protección jurídica específica de los datos individuales de las personas físicas y jurídicas, en el ámbito de la actividad estadística de las administraciones públicas.

La aplicación del principio del secreto estadístico comporta también la prohibición de actuar sobre la base de los datos personales, de utilizarlos para otras finalidades no estadísticas o ilegítimas y de posibilitar el cruce con datos de diversos ficheros.

En definitiva, existe un doble vínculo obligacional en el contenido jurídico del secreto estadístico: por una parte la obligación legal de declarar los datos para la realización de actividades estadísticas; de otra, el imperativo legal de mantenimiento del secreto estadístico y también la obligación legal de difusión pública de los resultados estadísticos.

1.1. Derecho a la información y derecho a la intimidad.

La prohibición de revelar datos individuales, a fin de proteger la intimidad de las personas, no puede ser incompatible con el derecho general a la información sobre los datos estadísticos, los cuales son indudablemente de interés social. La aplicación del principio del secreto estadístico requiere conseguir el equilibrio adecuado entre las necesidades de información de los diversos agentes sociales y la obligación de mantener la confidencialidad de los datos personales: se debe superar con la aplicación de medios técnicos y con el establecimiento de garantías jurídicas la posible oposición entre estos dos derechos constitucionales: derecho social a la información versus derecho individual a la intimidad, en este caso, por medio del mantenimiento del secreto estadístico.

1.2. Secreto estadístico y secreto administrativo.

Se produce a menudo una oposición entre secreto administrativo y publicidad de la actividad administrativa. La administración pública tiene un deber

de secreto en su actuación en diversos ámbitos que no puede colisionar con el derecho a la información representado en este caso por la transparencia administrativa. El secreto estadístico participa formalmente de las características de los secretos oficiales, pero se diferencia profundamente de ellos en el plano material. El secreto oficial tiene como finalidad la protección de la seguridad del Estado y el secreto estadístico tiene como objetivo la protección de la intimidad del ciudadano informante respecto a datos personales de comunicación obligatoria.

1.3. Secreto estadístico y secreto profesional.

El secreto estadístico se puede considerar como secreto profesional. Es fundamentalmente, una obligación específica de un colectivo concreto y se aplica al personal de los órganos estadísticos y al de otros servicios estadísticos de las administraciones públicas como un elemento de su régimen jurídico, a la vez que se hace extensiva a cualquier otra persona física o jurídica que entre en contacto o tenga acceso a los datos estadísticos individuales o individualizados, por razón de su participación en operaciones estadísticas.

2. El Elemento Subjetivo en la Figura del Secreto Estadístico.

2.1. Sujeto activo de la obligación.

Los sujetos vinculados por la obligación del mantenimiento del secreto estadístico son todos aquellos que trabajan en el ámbito de la actividad estadística y que tienen o pueden tener acceso a información que puede dar lugar a una revelación de datos personales.

Los sujetos activos de la obligación de mantenimiento del secreto estadístico son:

a) Los órganos titulares de la función estadística pública y otros servicios estadísticos de la administración, los cuales deben garantizar la confidencialidad de los datos que han obtenido en la realización de operaciones estadísticas amparadas por los beneficios legales correspondientes y de los que son depositarios y gestores.

b) Todo el personal implicado en la elaboración de las actividades estadísticas en cualquiera de sus fases: recogida de datos, tratamiento y difusión, sin distinción de su status profesional y laboral.

c) Las empresas y sus responsables, colaboradores y empleados, los profesionales y el personal investigador que mediante un convenio de colaboración o de una relación contractual no laboral, colaboren en la realización de una actividad estadística.

El deber del mantenimiento del secreto estadístico continua vigente para todo el personal obligado incluso con posterioridad a su desvinculación de aquellas actividades estadísticas a través de las cuales hubieran tenido conocimiento de los datos protegidos.

2.2. Sujeto pasivo de la obligación.

El sujeto pasivo de la obligación es la persona física o jurídica, titular de los datos individuales de declaración obligatoria, tanto si la información es de origen administrativo como de origen estadístico.

3. Ambito de Aplicación del Secreto Estadístico.

3.1. Objeto del secreto estadístico.

El objeto del secreto estadístico está constituido por los datos individuales recogidos, utilizados u obtenidos, tanto directamente de los informantes como a través de fuentes administrativas con fines estadísticos.

La regulación del secreto estadístico es aplicable tanto a los datos individuales o individualizados como a aquellos que permitan razonablemente la identificación individualizada de las personas físicas y jurídicas que hayan suministrado información de comunicación obligatoria, es decir, se aplica tanto a la revelación directa como indirecta de datos.

Está prohibida la divulgación o la comunicación de esta clase de datos por cualquier medio y a cualquier persona física o jurídica, incluidas las administraciones públicas, no sometidas a la obligación de mantenimiento del secreto estadístico.

Las disposiciones de regulación del secreto estadístico y la doctrina prevén excepciones a este principio general de prohibición: datos contenidos en registros públicos, datos de directorios, datos recogidos en publicaciones, acceso a datos con fines de investigación en el ámbito universitario, aceptación formal de revelación de datos por parte del titular, secreto pasivo, etc.

3.2. Vigencia temporal.

La obligación de mantener el secreto estadístico se inicia desde el mismo momento en que se obtienen los datos y puede tener un período de vigencia determinado, bien porque se establece una limitación temporal a partir de la cual los datos serían accesibles, bien fijando que a partir del transcurso de un determinado período de tiempo sólo ciertas personas puedan acceder a aquellos datos.

El período de vigencia del secreto estadístico no debería de ser el mismo para los datos que correspondan a personas físicas que para los que pertenezcan a personas jurídicas. En el caso de las personas jurídicas, el plazo de vigencia del secreto podría vincularse a las diversas vicisitudes de la vida legal de las sociedades.

3.3. Finalidad del secreto estadístico.

El secreto estadístico tiene una finalidad general derivada de su propio fundamento jurídico: la protección de la intimidad de las personas, y una finalidad específica, íntimamente ligada a la actividad estadística pública: mejorar la calidad de los resultados de las actividades estadísticas a partir del aumento de la confianza de los ciudadanos y, por tanto, de la sinceridad en las respuestas.

Los Derechos de las personas en la LORTAD

GUILLERMO OROZCO PARDO
Profesor Titular del departamento de Derecho Civil de la Universidad de Granada.

I. Introducción.

1- Una perspectiva socio-jurídica.

Estas líneas están dirigidas a apuntar un primer análisis de los derechos consagrados en la nueva Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter Personal (L.O.5/92 de 29 de Octubre) texto que, por reciente, aún no ha sido desarrollado reglamentariamente en su totalidad ni tampoco ha sido objeto de una interpretación y aplicación por parte de nuestra Jurisprudencia. Ello supone una dificultad importante para su estudio de tal suerte que todo análisis científico conlleva el riesgo de avanzar tesis y propuestas a veces arriesgadas, de tal suerte que nuestra labor se nos antoja un "paseo por la cuerda floja", pues el investigador está acostumbrado a contrastar teorías y utilizar pluralidad de fuentes del conocimiento que en este caso no poseemos, mas que las relativas al desarrollo del tema en otros países. No obstante, nos consta que un grupo cada vez más amplio de juristas e informáticos están desarrollando su labor científica en esta materia pues incluso existen ya Tesis Doctorales en pleno desarrollo. Ello contrasta con la situación

en el campo legal, jurisprudencial y científico de otros países de nuestro entorno, Estados Unidos, Italia, Francia, etc... donde este tema ha sido ya objeto de regulación y tratamiento, aún cuando los materiales de estudio no sean tampoco abundantes, si cabe destacar a juristas de nuestro país cuya labor en este campo es especialmente importante. Esta circunstancia hace mas destacables aún las iniciativas como ésta de realizar un estudio omnicomprensivo de la LORTAD en el seno de esta Universidad. Quede claro pues de salida que nuestro estudio será necesariamente breve e incompleto, pues las posibilidades que la materia ofrece son muy superiores a los propósitos de este trabajo, por lo que rogamos la clemencia del lector.

La cuestión concreta que nosotros abordamos posee especial significado pues se trata de analizar algo tan importante como son los derechos que garantizan a la persona la defensa frente a posibles abusos y lesiones que pueda sufrir como consecuencia de la utilización ilícita de los medios informáticos. Tales perjuicios pueden lesionar no sólo su intimidad u honor, sino que afectan también al libre ejercicio de sus derechos; es decir que se trata de disponer de unas garantías que protejan globalmente a la persona, en cuanto individuo, como miembro de una unidad familiar y en su faceta de ciudadano. No se trata ya del "egoísta derecho a estar solo" basado en una concepción excesivamente individualista de la persona, sino del derecho a un libre desenvolvimiento de la personalidad sin intromisiones ilegitimas en su esfera personal, tanto individual como social. Ya en el Siglo XVIII se afirmaba que el hombre "cede" parte de su libertad en beneficio de obtener seguridad, protección y colaboración por parte de la comunidad a la que pertenece. Hoy la sociedad debe poseer información sobre los ciudadanos y sus circunstancias en la medida en que sea preciso en orden a la planificación económica, la política fiscal, la prevención protección social y sanitaria, la seguridad frente al delito, la defensa o el ejercicio de los derechos de los ciudadanos, imponen la necesidad de esa acumulación de información y es por ello que cabe afirmar que todo derecho cumple una función social y debe ejercitarse evitando conductas abusivas por parte de su titular que cede parte de su libertad y su esfera privada en aras de la colaboración social; sería la "Razón de Estado" como fundamento del conocimiento de datos pertenecientes a los ciudadanos. Por otra parte, el particular en sus relaciones con los demás precisa adquirir y ceder información para desenvolverse en el tráfico jurídico-económico o en sus relaciones sociales. Así, circunstancias como gravámenes reales en inmuebles, descubiertos financieros, régimen económico, estado civil, dirección y teléfono, etc..., se hacen precisos en determinadas circunstancias y para ello se crean instrumentos de publicidad como Registro Civil, de la Propiedad, etc... accesibles a todos, salvo ciertas restricciones, legalmente establecidas, de tal forma que su desconocimiento no sea excusa para el afectado. Por otra parte, la información

es hoy un instrumento de poder a la vez que una "mercancía" de valor creciente y en el mercado de bienes y servicios resulta hoy imprescindible; como consecuencia de ello surgen los medios de almacenamiento y tratamiento automatizado de esa información y, lógicamente, surge el abuso. La difícil tarea que la Ley se impone, entre otras, es asegurar una esfera privada a la persona que no pueda ser invadida sin su consentimiento, salvo casos excepcionales legalmente previstos y fundados en una causa justa.

Es ya tópico el comparar la invención de la imprenta con la de la informática, si bien las consecuencias de ésta son mucho más amplias e imprevisibles, pues ningún invento precedente (salvo la energía atómica) dota a su detentador de unas mayores posibilidades de conocimiento y control de los ciudadanos. Es por ello que afirma Pérez Luño: "El signo distintivo de nuestra época es que en ella el progreso tecnológico se halla inescindiblemente ligado a elecciones o valoraciones éticas y políticas". Las posibilidades de utilización desviada son tales que se hace preciso "limitar" el uso de los medios informáticos, estableciendo unos principios jurídicamente consagrados y construir un sistema de garantías que permitan al afectado obtener una protección eficaz frente a lesiones a sus derechos y sancionando al infractor, y evitar lo que Davara denomina la "dictadura tecnológica". [1] Téngase en cuenta que el problema es que no sólo se han de impedir intromisiones ilegítimas en la esfera privada, sino evitar que datos lícitamente obtenidos sean utilizados o transferidos sin base legal; evitando así lo que se ha llamado "el rumor informático" ("noise") evitando la "diabólica combinación de palabras" que se origina por la cantidad de datos recabados de una persona y que no son objeto preciso de la finalidad para la que se recaban, frente a lo cual se erige el llamado "derecho al silencio". [2] Incluso, se impone una doble vertiente de responsabilidad al titular del banco de datos: diligencia en el mantenimiento de la "calidad" del contenido de la misma, en términos de veracidad, licitud y caducidad, y la obligación de responder por las consecuencias lesivas que su negligencia, en términos de responsabilidad objetiva, pueda ocasionar al afectado.

Es necesario establecer una coordinación ética, consagrada en la norma, que concrete qué **información puede recabarse, quién** puede adquirirla, bajo qué **condiciones** puede almacenarse, para qué **fines** se utiliza, si puede **trasmitirse** y **cuándo** ha de ser eliminada. Responder a tales interrogantes es esencial para un Estado democrático de Derecho, y para ello se pueden utilizar distintos sistemas, tal y como veremos en lineas posteriores, si bien todos ellos

■ 1- Vid. Pérez Luño, A.E.:*"Derechos Humanos, estado de Derecho y Constitución"* Madrid, Técnos, 3ª ed. y Davara Rodríguez, M.A.:*" Derecho Informático"*. Pamplona, Aranzadi, 1993 pág. 85 y ss.

■ 2 - Vid. Panuccio, V en: *"Banche de dati e diritti della persona"*. Milano, CEDAM, 1985. pág.82 y Lindon, R.: *"Dictionaire juridique: les droits de la personnalité "*. Dalloz, París, 1983, muy útil para conocer la jurisprudencia y la Ley francesa.

basados en un eje central: la persona, en sus múltiples facetas, y sus valores, poniendo a su disposición mecanismos previos de control para conocer y decidir qué datos relativos a ella son recogidos y almacenados y prestar su consentimiento para ello. Estos supone estar informado de la existencia del fichero, de su contenido, acceder a él y poder exigir la rectificación o cancelación del dato inexacto o improcedente, cuando así proceda. En ello subyace una doble vertiente del interés jurídicamente protegido: el interés particular del sujeto afectado y su libertad de decisión y el interés colectivo que precisa dotar de seguridad a las informaciones que se almacenan son procedentes, veraces, adecuadas a la finalidad lícita perseguida y son legítimamente adquiridas por los cauces legalmente establecidos.

2- El análisis civilista.

Con frecuencia, del análisis de un texto legal se deducen muchas mas cuestiones de las que en una primera lectura pudieran deducirse; ello se debe a que la norma es el instrumento básico para regular conflictos de intereses, y éstos son de diversa naturaleza. Esto hace necesario evitar la "rigidez" de las normas, para ello el legislador utiliza conceptos "standard" tales como buena fe, diligencia debida, realidad social, etc... que permiten adaptar la aplicación de las normas a la evolución de las circunstancias de la sociedad. Esta evolución supone la aparición de fenómenos nuevos que originan conflictos no previstos y ante los cuales es preciso tener que desarrollar normas especiales con los riesgos que ello conlleva. Incluso puede suceder que normas cuya meta es regular un fenómeno en concreto, así la LORTAD, no contemplan la totalidad de las cuestiones que se suscitan, por lo que el jurista viene obligado a "completar" esa regulación acudiendo a otras normas del Ordenamiento cuya aplicación resuelve el conflicto no regulado, a la vez que nos aportan criterios interpretativos de la norma especial. Esta es la gran tarea del civilista: utilizar su conocimiento de las normas del ordenamiento para interpretar y completar la LORTAD a la hora de resolver las cuestiones, previstas o no en ella, planteadas por el objeto de la misma. Dicho objeto esta constituido por la informática en cuanto técnica y la finalidad perseguida por la norma es más que limitar su uso, consiste en **regular** todo el conjunto de relaciones que de la utilización de tales medios se deduce para garantizar a la persona el libre ejercicio de sus derechos, sean de carácter personal o patrimonial, y el respeto a sus valores y atributos esenciales, poniendo a su disposición unas garantías como medio de hacer valer tales derechos. Su flexibilidad se pone de manifiesto al utilizar "standards" tales como datos personales o privacidad, y la primera labor del jurista será interpretar tales conceptos dotándoles del contenido que la sociedad en cada momento les asigne; en segundo lugar, debe el jurista analizar qué cuestiones no están

resueltas en la norma y acudir al ordenamiento jurídico para obtener la norma aplicable que resuelva el conflicto no previsto.

Los bienes jurídicamente protegidos afectados por la informática no sólo son los de carácter personal, como la privacidad, sino que también los hay de carácter patrimonial: el usuario de los bienes y servicios que se prestan, así ficheros automatizados públicos o privados, ostenta aquí plenamente su "status" jurídico de consumidor y por tanto le serán de aplicación las normas de Derecho del Consumo y los derechos que en ellas tiene reconocidos. Por otra parte, el prestador del servicio, titular del fichero, posee su propio estatuto que, en parte se integra por normas de la propia Ley (así todo el Capitulo II) y también por otras normas, tales como las relativas a su responsabilidad civil o las penales que sancionan ciertas conductas.

De todo lo que antecede se deduce paladinamente que la materia posee múltiples aspectos que interesan al Derecho Civil en cuanto éste posee como valor y objeto central la persona y sus valores y no un exclusivo acento en lo patrimonial como pudiera parecer de una lectura superficial. Es más, al haberse acentuado el matiz social de la persona, y por ello el contenido y función de los derechos a ella inherentes, la disciplina civilística ha evolucionado en los últimos tiempos en sus contenidos y principios de una forma paralela a la sociedad. Efectivamente, temas como función social de la propiedad, el abuso del derecho, el derecho de uso inocuo, el moderno Derecho de daños, basado en la responsabilidad objetiva, el derecho del consumo, etc... supone el abandono de posiciones individualistas para consagrar una concepción mas social y solidaria de la persona, sus derechos y sus deberes, pero sin que ello suponga desde luego una "desprotección" de la misma, por cuanto se avanza en un catálogo abierto de derechos a ella referidos que se enriquece hoy con los de matíz social, económico y culturales, así el derecho a la cultura, al medio ambiente o a la solidaridad social frente al daño, son patentes pruebas de ello.

Es por ello que la "revolución informática" no puede ser ignorada por el jurista, ya sea teórico o práctico, pues debe adecuar los criterios y medios de investigación a la evolución de la realidad social, pues de lo contrario queda marginado por obsoleto. Incluso se supera la tradicional dicotomía entre la esfera teórica y la práctica ya que cada vez se acentúa mas la certeza de que el derecho es una ciencia eminentemente práctica, que se dirige a resolver conflictos de intereses, en base a la interpretación de la norma mediante unos criterios socialmente compartidos, por ello el jurista desarrolla su labor en un campo operativo en el que confluyen teoría y práctica. Por ello precisa de una especial sensibilidad y un conocimiento profundo de tales criterios sociales y de esa realidad sobre la que opera para conformar una experiencia jurídica de

deducir la solución al conflicto planteado; en razón de lo cual se afirma que no hay nada más práctico que una sólida construcción teórica.

Sin embargo, el ordenamiento jurídico no dispone siempre de normas que solucionen las situaciones de conflicto que la realidad va planteando, pues el Derecho suele ir por detrás de ella, y ello produce en ocasiones la "quiebra" de la certeza del Derecho, y por ello, de la seguridad jurídica. [3] En tales casos la Jurisprudencia y la Doctrina están llamadas a realizar una difícil labor: dar solución previa a una problemática no resuelta por el legislador. Para ello la técnica interpretativa y sus medios se convierte en un mecanismo esencial en la resolución del conflicto; la reiteración de esa solución se acaba consagrando en la norma, sea legal o consuetudinaria. En tal caso, es primordial perfilar claramente cuál es el valor o bien protegido sobre el cual se investiga, así como delimitar los principios, criterios y técnica a aplicar, y en nuestra perspectiva civilística ese "centro de gravedad" es la persona, tanto en su faceta individual como social, es decir, un concepto en el que se sintetizan lo privado y lo publico, conciliando ambos aspectos e intereses, asegurando a la vez una esfera privada de desarrollo de su personalidad y su participación en la comunidad aceptando intromisiones legítimas, para lograr una "ósmosis" armónica entre ambas esferas. [4]

Es en este contexto en el que debemos analizar la disciplina de la protección de la persona y su esfera de actuación, teniendo en cuenta que los límites entre ambos campos han sufrido un cambio dimensional. A tal efecto se cita como ejemplo el de las sentencias y su contenido pues siempre se entendieron como un acto público accesible a todos, por el principio de ejemplaridad de la pena. Sin embargo, merced a las posibilidades que su tratamiento automatizado ofrece hoy, se ha generado un fuerte rechazo en ciertos ámbitos ante la posibilidad de acceder a ellas y tratarlas por medios informáticos, tal y como veremos en líneas posteriores. Por tanto, establecer los límites de lo público y lo privado en la esfera personal es tarea complicada que debe resolverse en el caso concreto, pues no caben respuestas apriorísticas generalizadas, pero

■ 3 - Sobre el tema véase Pérez Luño, A.E.: *"La seguridad Jurídica"*. Barcelona, Ariel, 1991

■ 4 - Por ello afirma Pérez Luño: "Puede inferirse de estas orientaciones teóricas actuales que la intimidad en la pluralidad de sus acepciones está en directa e insoslayable relación con otros valores (dignidad, libertad, libre desarrollo de la personalidad, autodeterminación, etc...) que tales valores no constituyen categorías axiológicas cerradas y estáticas, pues cuanto más se profundiza en el significado de cada uno de ellos más evidente resulta su interdependencia con los demás, y que la intimidad, lejos de implicar autoconfinamiento del sujeto moral, supone su incorporación a un proceso de estímulos y proyecciones sociales. Si es cierto que cada hombre debe tomarse como fin en sí mismo, no lo es menos que ningún hombre puede alcanzar plenamente sus fines sólo por sí mismo. El libre desarrollo de la personalidad constituye un ejercicio cotidiano de **mitsein**; no es una aventura solitaria sino una forma de **con-vivir**". Vid.:" Intimidad y protección de datos personales: del Habeas Corpus al Habeas Data". En: "Estudios sobre el derecho a la intimidad". Ed. de Luis García San Miguel, Madrid, Técnos, 1992, pág.39.

teniendo siempre en cuenta el evitar que a través del uso abstractamente lícito de un instrumento pueda llegarse a resultados objetivamente ilícitos. Por ello se parte de unos principios de la protección de datos y se establecen unas categorías especialmente restringidas de datos cuya adquisición y tratamiento están sometidos a fuertes controles y restricciones, son los llamados datos sensibles, que abordamos mas adelante.

Como consecuencia de lo anterior, la disciplina civilista se ve compelida a revisar las categorías jurídicas tradicionales relativas a la protección de la persona y sus valores, partiendo de los criterios actualmente consagrados en distintas fuentes, tales como la Constitución de 1978 y en base a los fundamentos de un moderno Estado democrático de Derecho. Como la propia Ley indica, el artículo 18.4 CE no sólo pretende proteger la esfera de valores de lo estrictamente privado en relación con el honor, la fama o la intimidad, sino garantizar la **libertad** para posibilitar el libre ejercicio de los derechos, que todos ellos sean estrictamente individuales o de matiz social, pues se ostentan en cuanto persona y ciudadano. Para ello debe hacerse algo más que consagrar derechos, se deben crear las condiciones reales que posibiliten su ejercicio, es decir, dotarles de los mecanismos coercitivos necesarios para su efectiva operatividad. Así, conceptos tales como derecho subjetivo, derechos fundamentales, situaciones jurídicas subjetivas, garantías jurídicas, o las modernas "class actions" cuya consagración en el campo jurídico es cada vez mas clara, han de ser reexaminados a la luz de estos nuevos parámetros socio-jurídicos para adecuarlos a la realidad actual y hacer que su carácter de instrumentos de protección de la persona y sus valores en sus vertientes individual y social, tenga una eficacia real en la práctica.

De otro lado, los **aspectos patrimoniales** de ese campo de relaciones deben ser también analizados teniendo en cuenta que estamos ante un tema en el que se ven implicadas materias ya citadas como responsabilidad, consumo, etc... En definitiva, estamos ante una problemática multidisciplinar, que implica el análisis desde distintos campos científicos lo cual hace la tarea más extensa y difícil de lo que en una primera lectura pudiera parecer.

3. Informática y Derecho.

Es cierto que la solución a un problema jurídico depende a menudo de la respuesta que se dé a cuestiones no jurídicas, y para ello se debe atender a las fuentes del conocimiento que resuelven tales cuestiones. Se ha escrito mucho ya sobre las repercusiones sociales de la informática pues han sido, son y serán de tal magnitud que el Derecho, en cuanto coordinación ética de las relaciones sociales y como técnica de resolución de conflictos, se ha visto compelido a

regular y resolver todos aquellos supuestos en los que el uso y abuso de los medios informáticos ha llegado a desbordarlo, pues se han producido lesiones de distinto orden a los bienes y derechos de las personas. Problemas tales como propiedad del "software", "virus informáticos", delitos perpetrados mediante la informática, etc..., son realidades que hoy preocupan a la sociedad y, por tanto, al Derecho. Ello comporta que el jurista, en sus distintos campos, doctrinal, jurisprudencial y práctico, se vea forzado a tener que dar una respuesta a dichas cuestiones. Como afirma Kaiser, el desarrollo de la informática ha suscitado, a la vez que la esperanza de una sociedad mejor informada, más prospera y más libre, serios temores por el mantenimiento del equilibrio de los poderes en las sociedades democráticas, así como por los derechos del hombre y las libertades públicas, se trata de un delicado problema: conciliar el poder estatal, el interés público, con los derechos inviolables de la persona, en base a un espíritu democrático y al Estado de Derecho. [5] Es por ello que nos unimos a las palabras de Frosini:" Se puede, por consiguiente, comprobar una progresiva "computerización" de la vida privada, no sólo en cuanto se refiere a la cantidad numérica de los individuos fichados, sino también respecto a la particularidad, siempre más detallada y precisa de las informaciones que les conciernen". [6]

La Doctrina ha señalado las distintas formas en que el Ordenamiento puede regular este fenómeno proponiendo varias soluciones:

1ª- Mediante un tratamiento dentro del ámbito **constitucional**, tal y como sucede en Portugal, Austria o España, en el campo de los principios y de los derechos fundamentales, desarrollado posteriormente en la legislación orgánica y ordinaria.

2ª- Otra posibilidad consiste en un tratamiento **globalizador**, mediante una Ley General de Protección de Datos, así Francia, Alemania o Suecia.

3ª- Mediante un enfoque de carácter **sectorial**, dictando normas diferentes para el sector público y el privado, o bien sólo para uno de ellos, como sucede en Estados Unidos o en Dinamarca.

■ 5 - Vid. Kaiser, P.: *"La protectión de la vie privee"*. Ed. Económic, París, 1984, pág.288. Así mismo, Pérez Luño,A.E.: *"Derechos Humanos, Estado de Derecho y Constitución"*. Madrid, Técnos, 1990, pág.345 y *"Nuevas tecnologías, Sociedad y Derecho"*.FUNDESCO, Madrid, 1987; Orlando Cascio, F.: *"Sulla tutela della riservatezza"*. En: *"Banche datti e diritti della persona"*.Ed.Giuffré, Milano, 1986, págs 247 y ss. y Frosini, V.: *"Human rights in the computer age"*. En Rv.Informática e Diritto, 1989, págs 7 y ss.

6 - Vid. Frosini,V.: *"Cibernética, Derecho y Sociedad"*. Trad. Salguero Talavera y Soriano Díaz, Técnos, Madrid, 1982, pág. 179. Sobre la multitud de fuentes de recogida de datos, véase Lindon, R. *"Dictionaire juridique: les droits de la personnalite"*. Dalloz, París, 1983, pág.123.

4ª- Por último, un tratamiento **específico** para temas y actividades concretos, así la Ley Sueca de Información crediticia de 1973.

Por supuesto que cabe la posibilidad de adoptar una fórmula en la que se combinen distintas posibilidades, consagrando constitucionalmente unos derechos y principios básicos y vertebrándolos a través de una Ley orgánica y normas desarrolladoras, tal y como ha sucedido en nuestro país, donde la experiencia en otros ordenamientos ha sido decisiva. La Doctrina más autorizada en nuestro país ya señaló cuáles deberían ser las directrices básicas que vertebrarán la estructura de la futura Ley:

- Una definición consagradora de los **principios básicos** que han de regir la utilización de los medios informáticos en los sectores implicados y que infundan la Ley desde la idea de dar una respuesta global a la problemática que el fenómeno plantea.

- Establecer con toda claridad cuál sea el **ámbito de aplicación** de esa norma, partiendo de la base de la necesidad de imponer el registro de las bases como requisito previo e ineludible para su legitimidad y para su regulación y control.

- Sistematizar los medios de adquisición y tratamiento de los datos, estableciendo cuáles pueden ser recogidos, asegurando su calidad, la seguridad de su tratamiento y el control de su trasmisión y eliminación.

- El reconocimiento de todo un ámbito de actuación de la **libertad informática** integrada por un complejo de derechos-garantías realmente eficaces y dotados de los medios coercitivos adecuados para su real eficacia, de tal suerte que la autodeterminación del sujeto frente al este fenómeno quede asegurada, tanto en la vía antiprocesal como por los Tribunales de Justicia. Tipificando taxativamente los supuestos de excepción al ejercicio de estos derechos, fundados siempre en una causa legitima afecta al interés general.

Es de destacar igualmente el Convenio de Protección de Datos del Consejo de Europa de 28 de Enero de 1981, ratificado por España en 1984, inspirado en las recomendaciones de la OCDE de 1981; así como las dos Propuestas de Directiva de la CEE sobre la materia de 1990. [7] El problema reside en que la

■ 7 - Vid. Benavides del Rey, J.L.: *"Aspectos jurídicos de la protección de datos"*. Rv.Fundesco, nº 38 de 1984. En el mismo número, véase Santo Domingo Garachana, A.: *"Una reflexión sobre el anteproyecto de Ley para la Protección de Datos"*, pág.5 y ss. El Convenio presenta desde luego importantes aportaciones de capital relevancia en cuanto a la calidad de los datos, su carácter de sensibles en ciertas materias, la seguridad de los registros y su control, los derechos de los ciudadanos de acceso, rectificación y cancelación y el interés general como fundamento de las limitaciones o excepciones al ejercicio de los mismos; si bien más complicado ha sido la virtualidad de su aplicación por distintos países, entre ellos el nuestro. Vid.

solución legal debe evitar la creación de una normativa tan rígida y formalista que impida la existencia y funcionamiento de los bancos de datos, tan útiles en muchos casos. De otro lado, las normas no han de ser tan flexibles e inconcretas que impidan su plena eficacia y aplicación. No se trata, por tanto, de un enfrentamiento o restricción de la informática en cuanto avance esencial de nuestra época, sino de controlar su utilización y sus fines. En definitiva, se trata de disciplinar el fenómeno bajo la perspectiva del control social y democrático de la informática, y de garantizar a la persona su capacidad de decisión y control sobre la existencia, contenido, utilización y fines de los ficheros y bancos que le afectan.[8]

De otro lado, nuestra Constitución como otras de su entorno, ya preveía los posibles abusos y peligros que la informática podía generar, por lo que en su artículo 18.4 vincula este fenómeno a contenidos tan elevados como los del Título Primero: los derechos y deberes fundamentales. En concreto, en su Capitulo 2° "de los derechos y libertades" , al ocuparse de derechos fundamentales tan esenciales a la persona como el honor y la intimidad, entre otros, establece en el párrafo 4° del artículo 18 como una **"garantía"** de la esfera privada de libertad del individuo y de sus bienes jurídicos tan esenciales como los antes mencionados. A tenor de dicho precepto, "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*". Este precepto implica un mandato ineludible al legislador para que establezca los mecanismos legales precisos a fin de crear las condiciones necesarias para que tales garantías resulten real y efectivamente aplicables. Castell, al comentar este artículo afirma: "En la mente y en la intención de los autores del 18.4, se denotaba la voluntad, no del todo explícita, de *embridar una potente innovación tecnológica,* que explotaba por doquier con creciente fuerza", sin embargo, critica la redacción y alcance del precepto: "La pretensión de establecer garantías de control de los controladores, encubría **la falta de alcance de la formula adoptada finalmente**".[9] El precepto liga así la limitación informática al campo individual representado por la "privacy", dejando a un lado afrontarla desde el plano social e institucional,

los mismos; si bien más complicado ha sido la virtualidad de su aplicación por distintos países, entre ellos el nuestro. Vid. Frosini, V. en *"Informática y Derecho"*. Trad. J. Guerrero y M. Ayerra, Temis, Bogotá, 1988, pág.161 ss. y Pérez Luño, A.E.: "Derechos Humanos..." cit. pág. 366 y ss., al que hacemos referencia cuando hablamos de la "doctrina más autorizada". Sobre la LORTAD véase Actualidad Informática Aranzadi nº 7 de 1993 y en el mismo número, Páez Mañá, J: *"La incidencia de la LORTAD en los procesos de producción y distribución de ficheros"*; del Peso Navarro, E.: *"La LORTAD, breve apunte a un Proyecto de Ley. El derecho a la Intimidad de la Persona"*. Rv. Base Informática, ALI, nº 21 de 1992, pág.31 y ss.

- 8 - Vid. Clarizia, R.:*"La proposta del progetto Mirabelli per la tutela della riservatezza"*. En: *"Banchi di Datti e Diritti della Persona"*. CEDAM, Padova, 1985, págs. 128 y ss.
- 9 - Vid. Castell Arteche, J.M. *"La limitación informática"*. En: *"Estudios sobre la Constitución Española"*. Hº a García de Enterría, coordinador Martín Retortillo, Cívitas, Madrid, 1991.

tal y como ha señalado la doctrina, con lo que el tema de la protección de datos no se aborda desde ambos planos cruciales; además Pérez Luño pone de manifiesto la **fractura** que supone la descoordinación entre los artículos 18.4 y 105.b C.E., dado que éste reconoce el derecho de acceso a los bancos de datos públicos dando a entender la posibilidad de una regulación diferenciada del mismo derecho con respecto a los bancos de titularidad privada, cuando en realidad la LORTAD comporta una regulación unitaria.[10] Sin embargo, existen normas como el artículo 1-b de la Proposición de Ley de Colombia sobre la protección de la "privacy", en la que expresamente se fija como uno de los objetos de la misma "democratizar el poder informático". [11]Con su ubicación en el artículo 18 se vincula el fenómeno de la informática al campo de los derechos fundamentales de la persona, lo cual tiene como primera consecuencia que la legislación desarrolladora del precepto antes citado habrá de ser por fuerza una Ley Orgánica, con las consecuencias de tramitación y jerarquía que ello conlleva. [12] No obstante, esta afirmación no es unánime en la doctrina pues existen autores como Sempere Rodríguez cuya opinión difiere pues afirma que poniendo en relación los artículos 53.1 y 81 de la CE, la reserva de ley ha de aplicarse sólo a la regulación de los derechos fundamentales y las libertades públicas, es decir, los comprendidos en la Sección 1ª del Capitulo 2º del Titulo 1º. Como consecuencia de ello dice: "En tanto en cuanto el desarrollo particularizado de los derechos consagrados en el artículo 18 imponga límites al ejercicio de otros derechos, aquéllos deberán ser regulados por ley orgánica, pero ello en ningún caso quiere decir que la materia en cuestión, en este supuesto el uso de la informática, deba ser regulado por ley". [13]Sin embargo, el legislador ha planteado la cuestión en sus términos exactos: estamos ante una norma cuyo contenido y finalidad entran de pleno en un campo reservado a regulación por ley orgánica, tal y como expresaba el artículo 1 del Proyecto y mantiene la Ley desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución y "tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar *de las personas físicas* y el pleno ejercicio de sus derechos". Mal podría cumplir tales tareas una norma de otro rango, pues su posición jerárquica le obligaría a ceder en determinados conflictos con otros derechos y normas de superior rango, tal y como sería el caso de la libertad de creación, estudio de investigación, práctica médica, etc...

- 10 - Vid. Pérez Luño, A.E.: "Derechos Humanos...". cit. pág. 365.
- 11 - Véase el análisis hecho por Losano, M.G.: "*Una proposta di legge sulla privacy nella Repubblica di Colombia*". R. Informática y Diritto, 1988.
- 12 - Sobre la cuestión véase la obra de Peman Gavín, J.: "*Las Leyes orgánicas: concepto y posición en el sistema de fuentes del Derecho*". En "Estudios sobre la Constitución Española. Homenaje al Profesor García de Enterría". Madrid, Cívitas, 1991, Tomo I.
- 13 - Vid. "*Comentarios a las Leyes Políticas*" EDERSA, Madrid, 1984, Tomo II, pág.436 y ss.

(véase el art. 10.7-b del Proyecto y artículo 10 de la LORTAD). De otro lado, su misión de mecanismo de garantía del pleno ejercicio de los derechos, así como del respeto a los derechos fundamentales, hacen necesario que su rango tenga la "fuerza" suficiente y paralela a tan alta misión. Es por ello que los derechos consagrados en esta Ley pueden entrar en conflicto con las facultades dominicales del propietario de los bienes informáticos, que están limitadas ahora en su ejercicio pues no pueden transgredirse los límites de "privacidad" y fines que la Ley consagra. Igualmente sucede con el principio de libertad de empresa: no cabe ya utilizar bancos de datos para almacenar contenidos que puedan suponer discriminación laboral, o contener datos de posibles clientes o que éstos no quieran que estén en poder de la empresa (vid. artículo 27 y 28 de la Ley). Además, nuestra Constitución recoge la limitación de la informática en su seno como una garantía que los poderes públicos tienen que proporcionar al ciudadano, tal garantía ha de ser respetada por el Estado y los particulares. Todo ello, hace que consideremos adecuado el desarrollo legislativo por vía de la Ley Orgánica, tal y como se ha hecho, no sólo por pura técnica jurídica, sino porque de lo contrario poca eficacia hubiese podido desplegar, además de obligar a un desarrollo fragmentado y parcial poco adecuado a la importancia del tema.[14]

De otro lado, es interesante resaltar dos cuestiones que la norma plantea:

La primera es la referente al hecho de que, en principio, al tratarse de derechos fundamentales la Ley se aplica a las personas físicas ya que son éstas las que, en puridad de conceptos, son titulares de los bienes jurídicos protegidos por aquellos derechos. Es decir, los datos *sensibles* cuyo almacenamiento y uso se pretende limitar y regular están referidos a las personas físicas, pero no a las jurídicas. No obstante, puede suceder que alguna de las conductas prohibidas por la norma afecte a personas jurídicas de distinta índole y que estas puedan verse afectadas por ello sin contar con un mecanismo defensivo adecuado a través de esta norma, si bien cabe utilizar la tutela de la acción aquiliana del artículo 1902 del Código Civil en un proceso declarativo ordinario. [15] En atención a ello, se preveía en la Disposición Final Tercera del Proyecto, ahora eliminada, que "el Gobierno, previo informe del Director de la Agencia de

- 14 - No obstante, determinados preceptos del Proyecto tienen carácter de Ley ordinaria en atención a su materia, tal y como establece la Disposición Final 5ª.
- 15 - Véase en este sentido Vidal Martínez, J.: "*El derecho a la intimidad en la Ley de 5 de Mayo de 1982*". Montecorvo, Madrid, 1984, pág.56 y nota 59; Pérez Cánovas, N.: "*Las personas jurídicas y el Derecho al Honor*". R.F. Derecho de Granada, nº 15 de 1988, pág.93 y ss. En el ámbito laboral existe, dentro del deber de buena fe, el llamado "deber de secreto profesional" que veda al trabajador toda conducta de transmisión o difusión de datos concernientes a su empresa que se consideren privados, máxime si conllevan una competencia desleal, ello se consagra en los artículos 72 de la Ley de Contrato de Trabajo y 498 y 499 del Código Penal. Véase Alonso Olea, M.: "*Derecho del Trabajo*". Ed. Un. Complutense, Madrid, 12ª edición. Lo mismo sucede con los funcionarios en los artículos 367 y 368 del Código Penal.

Protección de Datos, podrá asimismo extender la aplicación de la presente Ley a los ficheros que contengan datos referentes a las entidades, sociedades y otras personas jurídicas, en las condiciones que reglamentariamente se determinen". Esto no supone que la persona jurídica pase a adquirir la condición de sujeto titular de los derechos y facultades que consagra la norma, pues por esencia ello no es posible, pero para evitar lesiones inadmisibles por indefensión los mecanismos legales, debidamente adaptados, podrán ser extendidos para la protección de tales entidades. Contrasta la postura de la propuesta colombiana, antes reseñada, en el tema ya que el artículo 3-a) de la misma se alude a la tutela de las personas físicas y "personas jurídicas y entes naturales", teniendo estos últimos caracteristicas comunes con las personas jurídicas, si bien, como señala Guerrero Mateus, tales entes no llegan a adquirir personalidad jurídica, pero sin que ello sea obstáculo a crear situaciones jurídicamente relevantes. [16]

La segunda cuestión es la relativa a si dentro del ámbito subjetivo de la Ley debemos considerar incluidos, en base al término "ciudadanos", a los nacionales de nuestro país exclusivamente o, por el contrario, también a los extranjeros. El término ciudadano hace referencia a la idea de persona, no en cuanto sujeto individual, sino como miembro de una comunidad situado dentro de un marco de relaciones con los demás sujetos. Por ello cuando la CE utiliza el término no lo entiende como sinónimo de "nacional" cuando se está refiriendo a la titularidad de los derechos que son fundamentales en cuanto a su condición de persona, por lo que los extranjeros son también sujetos titulares de esos derechos constitucionalmente amparados. [17]En base a ello, debemos considerar que **toda persona física** es sujeto titular de los derechos consagrados en la presente norma, estando legitimado por ello para ejercitarlo mediante los cauces que reglamentariamente se determinaran, independientemente de su nacionalidad o cualquiera otra condición, (así, refugiados, transeúntes, etc... cfr. artículos 32 y 33 LORTAD).

Por otra parte, una Ley de estas características se ha de enfrentar a distintos problemas dándole unas soluciones de diversa índole. En primer lugar, debe establecer unos mecanismos de control de los medios informáticos, en segundo lugar, se han de consagrar un conjunto de derechos, de carácter sub-

■ 16 - Véase Guerrero Mateus, Mª F.: "*Osservazioni sulla proposta di legge sulla "privacy" nella Repubblica di Colombia*". R. I. e Diritto, 1989, pág.83 y ss. El artículo 196 del Anteproyecto de Código Penal aplica las disposiciones del Capítulo I, del Título IX : "Delitos contra la intimidad y el domicilio: de los delitos contra la intimidad y el secreto de las comunicaciones", al que descubriere o revelare datos reservados de *personas jurídicas* sin el consentimiento de sus representantes, salvo lo que dispongan otros preceptos del Código. Ello supondría un desfase entre la LORTAD y el nuevo Código Penal que puede "quebrar" la coherencia del Ordenamiento.

■ 17 - Véase el razonamiento de Sempere Rodríguez en lo relativo a los artículos 13.2 y 23.1 CE en su op.cit.

jetivo y de máxima jerarquía, que la persona puede ejercitar en defensa de su privacidad. De otro lado, deben crearse los mecanismos necesarios para hacer efectivo y eficaz el ejercicio de los mismos, arbitrando las medidas necesarias para sancionar su violación o la obstaculización de éstos.

El problema que nos ocupa se centra en la existencia y transmisión indiscriminada de bancos de datos, públicos y privados, cuyo contenido, titularidad y fines no son conocidos en muchos casos por las personas que en ellos figuran. Datos tan "sensibles" como salud, antecedentes penales, religión, estados civiles, situación económica, filiación política, etcétera, pueden estar almacenados, ser trasmitidos, incluso a título lucrativo, y ser utilizados con fines no siempre lícitos o, cuando menos, desconocidos o perjudiciales para el sujeto.[18] A tenor de la Constitución, la limitación del uso de la informática pretende evitar dos posibles daños diferentes: la lesión al honor e intimidad personal y familiar y el pleno ejercicio de sus derechos. En lo que a nuestro trabajo se refiere, debemos atender fundamentalmente al bien jurídico de la "intimidad", para precisar inmediatamente que este concepto no es el adecuado para el campo en que nos desenvolvemos, pues hoy la doctrina y el legislador han admitido ya el concepto de "**privacidad**" de origen anglosajón, ("privacy").[19]

De otro lado, se trata de la consagración a nivel legislativo de un conjunto de derechos subjetivos, referidos a la persona como individuo, como miembro del grupo familiar y como ciudadano, en el seno de los cuales el bien jurídico protegido viene referido a contenidos que afectan a distintos aspectos o esferas

■ 18 - Tal es el caso de las empresas que con fines comerciales almacenan el contenido de las resoluciones judiciales para elaborar listas en base a criterios de morosidad, sanciones penales, accidentes de tráfico, etc... que luego son vendidas a empresas y entidades bancarias y de seguros, para decidir, por ejemplo, la concesión de créditos o la contratación de trabajadores. Ello motivó que algunos jueces se negaran a facilitar el texto de sus sentencias a tales empresas, alegando el posible mal uso de su almacenamiento, lo cual contradice el esencial principio de publicidad de las mismas, tal y como declaró el Pleno del C.G.P.J. el 30 de Noviembre de 1990. Se trata de crear los mecanismos jurídicos necesarios al ciudadano para acceder y rectificar o cancelar, según el caso, el contenido de esa base de datos en lo referido a su persona.(Vid. diario "El País" de 1 de Diciembre de 1990, pág.29). Este interesante tema es objeto de estudio por Azparren Lucas, A.: *"Intromisión en el honor e intimidad de las personas por medio de las Sentencias"* en Actualidad y Derecho, nº 7 de 1992 donde afirma que "con carácter general se puede, por tanto, que las sentencias se encuentran exceptuadas por el artículo 8.1 (de la Ley 5 de Mayo de 1982) *no pudiendo considerarse ilegítimas las intromisiones al honor o a la intimidad divulgadas por una sentencia*". En el mismo sentido interpreta el Tribunal Supremo en su sentencia de 16 de Junio de 1989 el artículo 120.1 C.E. pues las resoluciones judiciales se entienden publicas. No obstante, el artículo 906 de la L.E.Cr. permite publicar las sentencias suprimiendo los nombres, lugares y circunstancias, e incluso las partes de la misma que puedan ofender a la decencia o atentar a la seguridad jurídica. Por tanto, establecer "bancos parapoliciales de conductas delictivas" de titularidad privada nos parece inadmisible de todo punto, por lo que el archivo informatizado de sentencias habría de realizarse bajo estricto control y, desde luego, sin contener datos de identificación de los sujetos implicados en los asuntos tratados en la sentencia. Incluso el artículo 7.7 de la Ley de 1982 considera intromisión la revelación de datos privados de una persona o familia *"conocidos a través de la actividad profesional u oficial de quien las revela"*, conducta esta que impide facilitar tales datos a profesionales, funcionarios y empresarios con destino a ficheros informatizados.

■ 19 - Se afirma que el origen del término está en la obra de Warren, S. y Brandeis, R.: *"The Right to Privacy"* publicada en Harward Law Review, en 1890. Vid. Wacks, R.: *"The Protection of Privacy"*. London, Sweet & Maxwell, 1980.

de su titular: antecedentes penales, situación familiar, salud, profesión, situación económica, religión, filiación política, etc... y cuyo conocimiento y difusión pueden o no interesar al sujeto o a la sociedad. Lógicamente, se antepone en ciertos casos el interés general como límite al ejercicio de estos derechos, así los datos necesarios para la Hacienda Pública o la Seguridad o Defensa Nacional. En otros supuestos, el almacenamiento de los datos se hace con fines estadísticos o de investigaciones sociológicas; o bien tales datos forman parte de la fase previa a una relación comercial: concesión de un préstamo o expedición de una tarjeta de crédito. El problema no es tanto la existencia de un banco de datos, como el conocimiento que el sujeto tenga del contenido que le afecta, de su veracidad, del grado de privacidad que comporten los datos, y del uso que de los mismos haga el titular de tales bancos. (Cfr. artículos 8, 21, 22, 30 y 33 LORTAD).

Las medidas a adoptar, básicamente, han de ser del siguiente orden:

- Un Registro que publique la existencia y finalidad de los bancos de datos, sean públicos o privados, para que su existencia sea conocida por todos, así como su titularidad y fines.

- Unas medidas de control de las personas que pueden tener acceso a tales bancos, sobre todo los que contengan datos "sensibles".

- Un código deontológico para el profesional informático que le dicte una "lex artis" de su profesión, en cuanto imperativo ético de conducta, que consagre una "clausula de conciencia" en la que éstos puedan apoyarse en ciertos casos, así como el deber de secreto y la responsabilidad por su incumplimiento tal y como hace la ley en preceptos como los artículos 9 y 10 donde se consagran el deber de adecuación técnica y seguridad de los datos y el de secreto, cuyo reverso sería el "derecho al silencio" que antes comentábamos.

- La prohibición absoluta de los abusos ocasionados por el "uso desviado" de los datos a fines distintos a los inicialmente previstos y constados. Ello implica la prohibición de las "listas negras" comerciales, laborales, políticas, etc... así como la transmisión comercial de los datos sin consentimiento del sujeto perjudicado (Cfr. arts 6, 11 y 28).

En el campo concreto de los derechos subjetivos, se trata del reconocimiento de un conjunto formado por el derecho de **acceso** a los ficheros y conocimiento de su contenido, el derecho a obtener la **rectificación** de su contenido cuando no se ajuste a la realidad, el derecho a la **cancelación** del contenido cuando éste afecte a datos sensibles que no puedan ser almacenados sino en

ciertas circunstancias y el derecho a ser **indemnizado** por las lesiones que tales abusos puedan producir, para lo cual la norma se remite parcialmente a la legislación penal. Básicamente la raíz de tales derechos se encuentra en esa libertad de autodeterminación frente al uso de la informática en relación con datos personales que implica otros derechos no formulados claramente en la Ley, tales como el de **silencio, olvido**, así como mecanismos previos: el consentimiento del afectado como máxima expresión de esa libertad antes citada y que consagra el artículo 6 de la Ley. Por tanto, no se trata de derechos aislados, sino de todo un sistema coherente y complementario formado por unos derechos subjetivos que actúan a modo de garantías jurídicas al servicio de un derecho fundamental: la libre autodeterminación frente a la recogida y tratamiento automatizados de datos de carácter personal. Tal y como el artículo 6.1 se consagra este mandato del 18.4 CE: es **requisito previo e ineludible** para el tratamiento automatizado de datos **el consentimiento del afectado**, "salvo cuando la Ley disponga otra cosa" expresión ésta peligrosamente inconcreta y, desde luego, bastante incorrecta en terminología jurídica. No obstante, tales derechos no son un catálogo cerrado, sino que la doctrina entiende que existen algunos no recogidos nominalmente en la norma, lo cual no es óbice para su existencia, por ello lo más adecuado es hablar de un derecho a la libre autodeterminación informática consagrado en el artículo 18 CE, núcleo esencial de todo un sistema de protección, en el que se integran a su vez una pluralidad o haz de facultades formadas por derechos subjetivos que actúan a modo de garantías para su efectividad.

II. Privacidad e Intimidad.

De la lectura del texto legal, se deduce la incorporación al campo jurídico de nuestro país de una serie de términos que, siendo fundamentales para una perfecta comprensión y aplicación de la norma, sin embargo no son fáciles de dotar de contenido exacto. En efecto, conceptos tales como los de *"privacidad"* y *"datos sensibles"* son nuevos en nuestro lenguaje jurídico y, sin embargo, relevantes a la hora de comprender la norma que los incorpora.

En relación con el término **"privacidad"**, cuyos orígenes han sido comentados anteriormente, su incorporación al texto fue criticada durante el debate parlamentario por considerarse ambiguo y poco definido, ya que pareció mas adecuado mantener el de "intimidad" cuyo contenido y alcance está mas perfilado. En el Derecho Italiano, el término "riservatezza" viene a hacer referencia a la contraposición de intereses entre los sujetos y el almacenamiento y difusión de datos o noticias concernientes a la vida privada de las personas. En el fondo, se trata del interés subyacente del sujeto por conocer y controlar las

informaciones que le conciernen, para evitar la difusión de aquéllas que pueden ser contrarias a sus intereses, su honor, etc... "Es un modo de ser que se contrapone a la publicidad", es un concepto que incluye notas psicológicas y sociales, como dice De Cupis es el modo de ser de la persona que consiste en la exclusión de los demás del conocimiento de cuanto hace referencia a la misma persona, es un "modo de ser negativo" de la persona con respecto a los otros sujetos, y más precisamente respecto del conocimiento de éstos. No está referida a su esfera física, sino al orden espiritual que consiste en la exigencia del aislamiento moral, a la no comunicación externa de cuanto atiende a la persona como individuo: es una cualidad moral de la misma basada en su "derecho a estar sólo".[20] En definitiva, se trata de tener acceso, conocimiento y disposición (¡control!) de lo que Romeo Casabona llama "**identidad informática**" para controlar el uso que se realiza de tales datos. Este mismo autor afirma: "Un breve exámen de la protección penal de la intimidad en nuestro Derecho revela que aquélla responde a concepciones ya superadas y parcelarias, *que resulta insuficiente y, por tanto, insatisfactoria,* ***y mucho más si la vulneración se produce por medios informáticos***". [21] De salida, nos parece decisiva la afirmación de Clarizia, en base al proyecto Mirabelli, de que en una sociedad informatizada la misma noción de intimidad se modifica, pues resulta ya insuficiente.[22] La idea de intimidad personal hace referencia a una esfera de la persona y de su actividad que se sustrae deliberadamente del conocimiento ajeno. Ello le vincula a otras facetas como el honor o la imagen, en cuanto se trata de un ámbito garantizado de la persona frente a intromisiones ilegítimas e inconsentidas por ésta. El propio consentimiento y el ámbito que por la propia conducta se reserva cada persona, son elementos delimitadores del alcance de este derecho, de acuerdo con las normas y usos sociales, lo cual se pone plenamente en evidencia en los casos de colisión con el derecho a transmitir información, tal y como afirma el T.C. en su Sentencia de 2 de Febrero de 1993, entre otras, donde mantiene su reiterada doctrina de que el honor y la intimidad no son únicamente límites a la libertad de expresión, sino que son derechos fun-

- 20 - Vid. *"I Diritti della Personalitá"*. En "*Trattato di Diritto Civile e Commerciale*", de Cicu y Messineo. Milano, Giuffré, Vol. 4º, 2ª edición, pág. 283.
- 21 - Vid. Romeo Casabona, C.M.: "*La reforma penal ante las nuevas tecnologías de la información*".R. I. e Diritto, 1987, pág. 115 ss. Véanse los artículos 194, 195 y 196 del Anteproyecto de Código Penal de 1992 donde se le encuadra dentro de los delitos contra "la intimidad y el secreto de las comunicaciones". En concreto el artículo 194.2 aborda la sanción para el que se apodera sin autorización de datos personales o familiares de otro registrados en ficheros o soportes informáticos. La pena se agrava si tal acto lo realiza una persona encargada o responsable del fichero, máxime cuando se difunden tales datos. El artículo 195 sanciona al que revela tales datos conocidos por razón de su cargo u oficio o cualquiera otra circunstancia o relación; expresamente se sanciona el incumplimiento del deber de secreto.
  En el 196 se aplica también al descubrimiento de o revelación de datos reservados relativos a personas jurídicas, como antes señalamos. Vid. Luzón Peña, D.M.: *"Protección penal de la intimidad y derecho a la información"*, en "Estudios..." cit., pág. 68 ss.
- 22 - Vid. op. cit. pág. 129; véase también LASARTE ALVAREZ, C.: "*Derecho a la Intimidad "versus" libertad informativa: la primacía constitucional de la intimidad*". En R. Tapia, nº 64 de 1992.

damentales en sí mismos y que la libertad de información no tiene carácter absoluto que haya de prevalecer siempre frente a aquéllos, sino que en cada caso debe establecerse una *graduación jerárquica del bien protegible según su importancia y atendiendo no sólo a la veracidad de la información, sino a que ésta se desenvuelva en el marco del interés general.* Está claro que se debe proceder a valorar si la información que se adquiere es o no pertinente para la relación o finalidad concreta del caso, o si por su relevancia o interés social es justificado el adquirirla, pues de lo contrario su tratamiento inconsentido supone una inmisión o perturbación inadmisible y sancionado por la norma.[23]

En todo caso estamos ante un concepto unitario con distintas manifestaciones, basado en la dignidad de la persona frente a distintos tipos de intromisiones que de una u otra forma afectan a su vida privada, a su honor, etc...[24] Sin embargo, es importante evitar una indeterminación del concepto como ha sucedido con el término anglosajón "privacy", en cuanto se ha fragmentado su unidad pues se utiliza para hacer referencia a problemas diversos tales como tranquilidad espiritual, derecho al aislamiento, nombre comercial, integridad física o mental, secreto profesional, etcétera, tendentes a reunir toda la gama de derechos y libertades de ámbito individual.[25] En definitiva, ello se conecta con otros términos como "reserva de vida privada", "esfera personal y familiar", que son análogos y pretenden evitar toda una gama de conductas lesivas contra la esfera privada personal y familiar del sujeto. Tales intromisiones varían desde la intromisión en el domicilio, escuchas telefónicas, violación de correspondencia, divulgación de noticias y cualquier otra forma de perturbación de la "paz doméstica". Se entiende que la privacidad es una necesidad básica, esencial para el desarrollo y mantenimiento de una sociedad libre, así como para la madurez y estabilidad de la personalidad individual. En consecuencia, estamos ante la base para la consagración de un derecho de toda persona frente a las agresiones contra sí mismo, su hogar, su familia, sus relaciones y comunicaciones con los demás, su propiedad y sus negocios. Así concebido, este derecho incluye la protección frente a utilizaciones no autorizadas de su imagen, de su identidad, su nombre o sus documentos personales.[26]

- 23 - Véase el análisis de Bustos Puche, J.E.: *"Los límites de los derechos de libre expresión e información en la Jurisprudencia"*. En: "*Estudios sobre derecho a la intimidad*" cit., pág.101 y ss.
- 24 - No es fácil hacer una clasificación de tales intromisiones, tal y como se deduce de la obra de Fariñas Matoni, L.: "*El Derecho a la intimidad.* Trivium, Madrid, 1983, pág.7; véase la sistematización que hace Orellana Rojas, G.: "*Informática y derecho a la intimidad*" en las Actas del II Congreso Iberoamericano de Informática y Derecho. Ed. CREI, Guatemala, 1989, pág. 137.
- 25 - Vid. Robertson, A.: "*Privacy and human rights*". Manchester University Press, 1973 y Belvedere, A.: "*Riservatezza e instrumenti d'informazione*". En "Dizionari del Diritto Privatto". Dir. N. Irti, Varese, 1980, Tomo I, pág.727.
- 26 - Vid. García San Miguel Rodríguez Arango, Luis: "*Reflexiones sobre la intimidad como límite de la libertad de expresión*". *En "Estudios sobre el derecho a la intimidad*", cit. pág. 15, así como el resto de los interesantes trabajos en esta misma obra y ss. Wacks op. cit. pág.7 y ss. En este caso es interesante el supuesto de divulgación de cartas sin permiso de su autor con el consentimiento del destinatario. Por ejemplo, el estudio de la correspondencia íntima de dos personas puede poner de

En todo caso, es evidente que este derecho posee múltiples matices que confieren a la persona un amplio ámbito de facultades. De un lado, una posibilidad de excluir a los demás del conocimiento de aquellos aspectos de su vida privada que considere restringidos a su esfera personal o familiar. Este sería el "modo de ser negativo" de que hablaban Carnelutti y De Cupis. De otra parte, su consentimiento expreso puede ser la razón que legitime el conocimiento o difusión de cualquiera de estos aspectos privados, sobre todo cuando la persona los facilita en el seno de una relación contractual. Sin embargo, como todo derecho posee unas limitaciones que circunscriben su ámbito y modalizan su ejercicio; el interés general representado por distintas razones que permiten unas "inmisiones o intromisiones legítimas": la seguridad del Estado, la prevención del delito, la investigación y tratamiento sanitarios, etc...[27]

Por otra parte, la jurisprudencia ha consagrado una postura que atiende a la mayor o menor relevancia pública de la actividad o cargo del sujeto, así como a sus hábitos y conducta personal, para establecer los límites de ese ámbito de exclusión del conocimiento de datos de la vida privada. En relación con la informática, el catálogo de intromisiones podría realizarse en los términos en que lo hace Orellana Rojas señalando una problemática entre informática y derechos en distintos ámbitos:

1º Aspecto individual:

a- Protección del derecho a la privacidad.

b- Derecho de acceso a los datos (el "habeas data" que citan Nibblett y Tchang-Benoit).

c- Derecho de la persona a ser informada de los datos registrados sobre ella.

d- Derecho de la persona interesada, a obtener la rectificación de los datos existentes sobre ella.

e- Derecho a que los datos se utilicen sólo para la finalidad concreta para la que fueron registrados.

manifiesto hechos o actitudes que no quisieron revelar, en tal caso el derecho a la libre creación intelectual del artículo 20.1.b CE no ampara esa publicación en cuanto que el respeto a los derechos fundamentales de terceros es un claro límite al mismo; pues incluso cabe plantearse la legitimidad de la autorización de los herederos o derecho-habientes.

■ 27 - No obstante, el debate del Proyecto ha puesto de manifiesto lo "discrecional" de tales límites, sobre todo en los bancos de datos policiales y de Hacienda. Véase el diario "El País", 15 de Mayo de 1991, donde algunos juristas tratan esta limitación de anticonstitucional.

f- Derecho a que se cancelen datos cuyo almacenamiento no sea consentido o carezca de legitimidad.

2º Aspecto institucional o social:

a- Determinación de los gestores de la informática.

b- Posibilidad de informática privada.

c- Control democrático de la informática.

d- Métodos a emplear en la elaboración de las informaciones.

e- Control y Registro de los bancos de datos públicos y privados.

f- Código deontológico de los informáticos.

3º Aspecto relativo a la protección del individuo frente a los abusos:

a- Organo especializado de la Administración.

b- Comisario Parlamentario, Agencia de Protección de Datos
Defensor del Pueblo.

c- Catálogo de infracciones, sanciones y penas.

d- Protección jurisdiccional.

Como puede verse, las implicaciones y demandas que la materia plantea a nivel legislativo, judicial y administrativo, son múltiples e importantes. A todas ellas pretende dar satisfacción la norma que comentamos, para lo cual parte del mandato constitucional, establecido en los términos que conocemos, pero con plena conciencia de las dificultades que ello ha de solventar. La primera de ellas consiste en que el concepto de intimidad no posee el ámbito objetivo necesario para contener todos los aspectos que la norma pretende proteger. Es por ello que el legislador, en la Exposición de Motivos, aborda la cuestión y nos da las razones por las cuales utiliza ya el termino *privacidad*.

Tras hacer alusión al mandato de nuestra Constitución, cuya modernidad hace que establezca tales garantías frente a la posible utilización "torticera" de la informática, lo cual tiene su origen en el desarrollo de las técnicas de recolección y almacenamiento de datos que pone a la *privacidad* ante una potencial

amenaza antes desconocida. Dice el texto: "Nótese que se habla de la **privacidad**, y no de la intimidad: *aquélla es más amplia que ésta*, pues en tanto que 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 ("la diabólica combinación de las palabras"), *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 CE y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo". Se trata, por tanto, de un concepto más amplio y globalizador de la esfera personal y familiar, que no se circunscribe a lo que hasta ahora entendíamos por "circulo privado" de la persona, sino de toda una serie de referencias a la misma que sirven para hacer una suerte de "retrato de su personalidad" personal, familiar y social: creencias, religión, salud, taras físicas o psíquicas, comportamientos sexuales, gustos y hábitos de consumo, profesión, propiedades y bienes, deudas pendientes, nivel salarial, nivel cultural y educacional, crédito comercial, etc... entran dentro de ese "supraconcepto" que es fuente de datos de la persona que permiten "retratarle" y obtener información útil para distintas finalidades, sin que el sujeto conozca tan siquiera que tales datos existen y están en posesión de terceras personas o entidades públicas o privadas. En definitiva, es mucho mas que el derecho a ser dejado solo, y por ello nos abonamos a la postura de Alpa en el sentido de que cuando se habla de intimidad, reserva, vida íntima o privada nos estamos refiriendo tan solo a un aspecto significativo, pero incompleto, del problema. Se entiende que aludimos a las intrusiones en la vida familiar y personal, a la intimidad de las actividades que se desarrollan entre las paredes de la casa, por lo que el daño sólo acontece en la medida en que se viola esta esfera de privacidad, ya sea por publicación de noticias reservadas, sea por difusión de datos personales "e custoditi con cura", o por el uso de las imágenes que se ofrecen al público relativas a aspectos de la vida privada destinadas a permanecer, por su naturaleza, en la intimidad. Por ello, las descripciones y definiciones que hoy se ofrecen sobre la intimidad son parciales y no adecuadas para afrontar el problema en su complejidad, tal y como pone de manifiesto la doctrina más reciente al hablar del derecho que confiere el control sobre todo lo que nos concierne, es decir, sobre **qué**, **cuándo** y **quién** puede conocer datos que nos conciernen.[28] Se trata de elaborar un derecho a la exclusividad del conoci-

■ 28 - En su sentido negativo, supone el derecho a no ser conocidos por los demás sino en la medida en que nosotros lo queramos, lo cual le hace, en cierto modo, "antipático", según García San Miguel en op. cit. pág. 18.

miento de aquello que pertenece a la vida privada, en el sentido de que nadie puede tomar conocimiento ni revelar aquello de esa esfera que el sujeto no quiere que sea conocido por los demás. Se trata de que la persona tenga un poder de control sobre el modo en que las informaciones son recogidas, sobre su contenido y veracidad y sobre el uso que de las mismas puede hacerse.[29]

El problema básico estriba en la falta de una figura jurídica netamente perfilada que diera acogida, como bien jurídicamente protegido, a tan complejo contenido. Por ello decía Rescigno que la pretensión general de una protección de la persona frente a la "indiscreción", no existía en las legislaciones modernas. "Por lo menos, no existe una formula amplia capaz de comprender todas las formas de agresión a la reserva". [30] Esta es la función y contenido del concepto de **privacidad** y prueba de ello es que actualmente multitud de ordenamientos contienen ya normas legales que la consagran y tutelan.[31] La estructura del termino en su origen norteamericano se compone de una doble faceta: "disclosural privacy", de un lado, e "informational privacy", de otro, que tratan de los dos aspectos que reviste el "asalto a la privacidad", la invasión de la esfera privada, la toma y registro de datos, su utilización ilícita y su difusión pública. Como dice Rodotá, privacidad significa soledad, aislamiento ("el derecho a estar solo"), intimidad, anonimato, reserva, discreción y por ello es un concepto que se proyecta sobre y frente a la colectividad, en el seno de la "aldea global".[32] Dice Alpa que no se trata de defender al hombre en su fortaleza, "su castillo", no es una cuestión de hermetismo o secreto, ni de asegurar la custodia de un espacio vital, sino de controlar la esfera de reserva que cada uno porta dentro de sí mismo y que aparece "transparentad" e inerme ante los medios y métodos de indagación organizada de los aparatos públicos y privados. Tampoco es posible, por otra parte, el recurso a la privacidad para ocultar datos de carácter económico, patrimonial o penal, impidiendo con ello aquellas formas de control social que tutelan los intereses de la comunidad.

Se trata, por tanto, de la defensa de la persona frente a la intromisión, la recogida, difusión y utilización de aspectos de su vida pertenecientes a su **privacidad**, actos que hoy son frecuentes y ante los cuales no podía oponerse un conjunto de instrumentos jurídicos eficaces. El aumento de este fenómeno se produce porque, como dice el Proyecto, "hasta el presente, las fronteras de la privacidad *estaban defendidas por el tiempo y el espacio*. El primero, procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas,

- 29 - Vid. Alpa, G.: "*Compendio del nuovo Diritto Privato*". UTET, Torino, 1985.
- 30 - Vid. Rescigno, P.: "*Persona e comunità*". Bologna, 1966.
- 31 - Así, Estados Unidos, Francia, Gran Bretaña, Italia, Austria, Australia, Japón, entre otros y Textos Internacionales y a nivel de la Comunidad Europea, suscritos ya por nuestro país.
- 32 - Rodotá, St.: *"Alla ricerca delle libertá"*. Bologna, 178.

impidiendo así la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. *El tiempo y el espacio operaban así, como salvaguardia de la privacidad de la persona*". El problema es que estos límites han desaparecido hoy, tiempo y espacio no son obstáculo para la informática que puede recoger, almacenar, procesar y cruzar datos de muy distinta índole, sea cual sea su lugar y momento de procedencia, sin conocimiento ni consentimiento de la persona afectada. Las posibilidades que ello comporta no escapan al legislador: "Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquella a la que sólo debe tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que autorice". Por tanto, el problema no es sólo la recogida y almacenamiento ilícito de los datos, sino que el riesgo es aún más grave: "El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor (se basa en la dignidad como afirma Fariñas); y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos". En definitiva, el concepto de **privacidad** establece una nueva frontera que garantiza aquél ámbito que contiene, para evitar que "un elemento objetivamente provechoso para la Humanidad, no redunde en perjuicio para las personas". La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 CE y al cumplimiento de ese objetivo responde la presente Ley".

III. Los Datos de Carácter Personal y los llamados Datos Sensibles.

Debemos plantearnos ahora cuáles son esos de carácter personal y, dentro de ellos cuáles serían **"datos sensibles"** que dotan de contenido a la privacidad y que lógicamente deben hacer referencia al ámbito de la misma. La ley considera como datos de carácter personal a "cualquier información concerniente a las personas físicas identificadas o identificables" (art. 3), pero dentro de esta amplia categoría debemos distinguir unos datos cuyo conocimiento y difusión ha de ser más reservado que el de otros, por lo que no cabe una respuesta unívoca a la hora de regular su tratamiento, por lo que se ha de distinguir la regulación según la "sensibilidad" de la información y su pertenencia a una esfera más o menos restringida de la vida y actividad del sujeto.

A tenor de la Doctrina, se entienden por tales, "prima facie", los datos relativos a la salud, vida sexual o convicciones políticas o religiosas, sobre los que no hay obligación de declarar, a tenor del artículo 16.2 CE. No obstante, señala Castell, "también se denotaba que datos perfectamente "anodinos" se descubrían de golpe como extraordinariamente *sensibles*, mediante un simple cambio del fin perseguido, cuestión fácil de llevar a cabo dada la extrema multifuncionalidad de dichos datos". [33] Ello pone de manifiesto que, en muchos casos un dato es inocuo o sensible, no ya por su contenido, sino por el uso que de él se haga, pues como señala el autor citado "la interconexión de ficheros, la libre utilización de los datos, producen la denominada teoría *del mosaico (Simitis), por el que datos "a priori" irrelevantes, pueden servir para una finalidad diferente y, por lo tanto, proporcionar claves insospechadas sobre una determinada persona*". En tal sentido, la postura más lógica, que sostiene la Jurisprudencia alemana, es la de no establecer diferencias entre los datos, atendiendo fundamentalmente al contexto y finalidad con que se utiliza. Por tanto, una norma eficaz ha de atender, no al contenido en concreto del dato desligado de cualquier otro elemento, sino utilizar criterios flexibles adaptables a los supuestos y contextos concretos del caso.

Toniatti hace unas distinciones partiendo de unos "datos personales irrelevantes o de rutina", sustraídos a este régimen normativo especial. Posteriormente, desde un punto de vista material entiende por *datos sensibles* "aquellos que más directamente se refieren sea a la esfera personal e íntima, sea a la titularidad de los derechos fundamentales de libertad", en tal sentido, cabe citar creencias religiosas, opiniones políticas, salud, antecedentes penales, origen racial, vida sexual, etcétera. Por último, habla de unos *"datos supersensibles o sensibilísimos"* para atender a una categoría especial en la que el ordenamiento excluye incluso al propio interesado y el ejercicio de sus medios de control para el acceso, corrección, etc..." Se trata esencialmente de datos personales clasificables desde el punto de vista material como datos ordinarios y sensibles que se cualifican ulteriormente por su presencia en archivos destinados a finalidades de orden particular y de valor preeminente, entre los que destacan, en primer lugar, la protección del orden público y de la seguridad nacional y, en segundo lugar, la intimidad en materia sanitaria".[34] Este es el espíritu que subyace en el texto del Convenio de 28 de Enero de 1981, ratificado por España (BOE 15 de Noviembre de 1985), pues además de atender al contenido de los datos, en función de los distintos grados de privacidad, atiende también

- 33 - Vid. Castell Arteche, J.S.: "*La limitación informática*". En "Estudios sobre la Constitución Española". cit., pág.924.
- 34 - Vid. Toniatti, R.: "*Libertad informática y Derecho a la protección de los datos personales: principios de legislación comparada*". Trad. Saiz Amaiz, R. V. A. P. nº 29 de 1991, pág. 139 ss. Véase igualmente Maisl, H., Simitis, Sp. y otros: "*Informatique et Droit en Europe*".Bruselas, 1985 y Madrid, F.: "*Derecho a la intimidad, Informática y Estado de Derecho*".Valencia, 1984.

al control de los métodos y fines de su registro y conservación, estableciendo unas garantías sobre información, acceso, corrección y borrado en favor de la persona afectada.

En definitiva, partimos de una categoría básica de datos sensibles atenientes a las materias ya citadas, si bien la limitación ha de extenderse a los procedimientos, medios y fines del registro de los datos, ya que datos inocuos, en principio, pueden servir para finalidad no admisibles. Por ello, no caben posturas unívocas sobre la cuestión, partiendo de unas materias y bases mínimas, sino que deben emplearse criterios flexibles que se adapten a supuestos concretos en atención a las circunstancias de cada caso.

La Ley recoge en su artículo 7 unos "datos especialmente protegidos" y atendiendo al precitado artículo 16.2 CE excluye la declaración sobre ideología, religión o creencias, sólo con el consentimiento expreso y por escrito del afectado puede hacerse un tratamiento automatizado de tales datos, previa información al mismo de su **derecho a no prestarlo**.

En segundo lugar, los datos relativos al origen racial, salud y vida sexual, sólo pueden ser recabados, tratados y cedidos previo consentimiento expreso (¿escrito?) del afectado o cuando así lo permita el interés general previa disposición legal al efecto. Esto quiere decir que la excepción a la prohibición sólo puede provenir o de consentimiento expreso o por una norma destinada al efecto basada en que ello sea afecto al interés general, por ello quedan prohibidos los ficheros cuya única finalidad sea almacenar datos sensibles de este tipo. Otra cuestión interesante es el hecho de que los datos penales por la comisión de infracciones penales o administrativas "sólo podran ser incluidos en ficheros automatizados de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras", ello debe ponerse en coordinación con los ficheros privados de "morosos" recogidos en el artículo 28 y con el almacenamiento de resoluciones judiciales sobre delitos económicos, pues del artículo 7.5 puede deducirse la ilegalidad de muchos de ellos.

En cuanto a los datos relativos a la salud, los centros e instituciones sanitarias y los profesionales pueden llevar a cabo el tratamiento automatizado en la medida en que sea preciso para el tratamiento, pero su cesión ha de contar siempre con el consentimiento del afectado, salvo en las excepciones previstas en el artículo 11.

El consentimiento ha de ser previo, expreso y tiene carácter revocable, prestándose para cesionarios determinados y para finalidades constatadas,

pues en otro caso es nulo; ello permite afirmar que este consentimiento es una manifestación de voluntad a la cual hemos de aplicar la teoría civil de los vicios del consentimiento, exceptuando los casos previstos por la misma ley autorizando la recogida, tratamiento, cesión sin consentimiento en los casos legalmente establecidos.

IV. Los Derechos de las Personas.

Nos encontramos ahora con la más importante de las aportaciones que la norma introduce. No se trata ya de meras técnicas limitativas o sancionadoras, sino que el legislador ha querido dar carta de naturaleza a unos **derechos subjetivos** de carácter personal atribuidos a todas las personas físicas. Estamos ante instrumentos que se constituyen en medios de protección y garantía de la privacidad de todo ciudadano frente al abuso informático. En la Exposición de Motivos, el Legislador nos dice ya cuál es la importancia que a tales derechos les confiere la norma: "*Las garantías de la persona* son **los nutrientes nucleares de la Parte General,** y se configuran jurídicamente como **derechos subjetivos** encaminados a hacer operativos los principios genéricos. Son, en efecto, los derechos de **autodeterminación, de amparo, de rectificación y de cancelación**, los que otorgan la virtualidad normativa y eficacia jurídica a los principios consagrados en la Parte General, *principios que, sin los derechos subjetivos ahora aludidos,* ***no rebasarían un contenido meramente programático***". Queda patente ya cuál es el rango y la importancia que tales derechos vienen a poseer dentro de nuestro Ordenamiento pues suponen el más eficaz instrumento puesto al servicio del sujeto para la defensa frente a la lesión a la vez que instrumento de control ciudadano, democrático, de la informática en lo relativo a bancos de datos y su utilización. Es más, como dice la Ley, tales derechos *"se constituyen como piezas centrales del sistema cautelar o preventivo instaurado por la Ley*". El llamado *derecho de acceso* tiene incluso plasmación constitucional en lo que se refiere a los datos que obran en poder de las Administraciones públicas, a tenor del artículo 105.b C.E., lo cual hace que la norma lo recoja con toda rotundidad, admitiendo sólo excepciones tales como la seguridad y el cumplimiento de la obligaciones tributarias, y ello como consecuencia de que tales excepciones están fundadas en el mismo texto constitucional y en el Convenio Europeo para la protección de los derechos fundamentales. Incluso, este derecho esta regulado dentro de la normativa reguladora de los Registros y Archivos administrativos, tal y como veremos después. En definitiva se trata de instrumentar un conjunto de derechos al servicio de otros derechos de carácter fundamental, para establecer "un nuevo y más consistente derecho a la privacidad de las personas". En su Título Tercero: "Derechos *de las Personas*", consagra la norma tales derechos partiendo de la base de su carácter personal, esen-

cial a toda persona física afectada por el tratamiento automatizado de datos que le conciernen, a tenor de lo establecido en el artículo 3, sin olvidar lo que antes dijimos con referencia a las personas jurídicas. No obstante, la categoría de tales derechos no queda circunscrita a los recogidos en dicho Título, sino que existen otros derechos dentro de la misma Ley aun cuando figuran consagrados en otros Títulos de la misma, tal y como sucede con el derecho de **Información** en la recogida de datos (art. 5), el derecho al **silencio** (art.10) y, sobre todo, el derecho a la **libre autodeterminación** informática en virtud del cual el libre consentimiento de la persona le asegura una esfera de decisión fundamental y al servicio de éste se consagran todos los demás, a modo de garantías jurídicas que le aseguran una acción frente a las conductas que lesionen tal derecho. Así lo entiende el Legislador cuando dice: "El principio de consentimiento o de **autodeterminación** otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes. Su base está constituida por la exigencia de *consentimiento consciente e informado* por el afectado para que la recogida de datos sea lícita", como afirma Gulleford, se trata de un derecho a conocer y decidir qué datos son recogidos y para qué finalidad.[35] Este derecho juega un papel fundamental "ab initio" pues la recogida de datos, en el caso de los sensibles, ha de hacerse previo consentimiento expreso, por escrito a veces, del afectado o en base a una habilitación legal fundada en el interés general. El mismo consentimiento juega en el caso de la cesión de datos de un fichero automatizado, informando al sujeto del uso que pueda dársele al mismo.

La primera cuestión importante estriba en el hecho de establecer la naturaleza jurídica de tales derechos. El legislador, sin más explicaciones, los incluye en la categoría de los derechos subjetivos. Como decía Del Vecchio, en todo derecho de este tipo subyace un elemento interno: una posibilidad de querer o hacer, y un elemento externo: una posibilidad de exigir a otros el respeto al mismo. [36] Ese poder, en su doble vertiente, pasa a constituirse como elemento esencial del concepto, por ello decía De Castro que estamos ante "una situación de poder concreto concedida a la persona, como miembro activo de la comunidad jurídica y a cuyo arbitrio se confía su ejercicio y su defensa. [37] En todo caso, la conexión entre derecho subjetivo y libertad se acentúa en las nuevas tendencias pues la teoría de las situaciones jurídicas subjetivas parece haber perdido vigor, aún cuando en ciertos casos siga siendo aplicada.[38] No obstante, la vinculación del derecho subjetivo con el concepto de *acción* en

- 35 - Vid. "*Data protection in practice*". Butterworths, Londres, 1986, pág.72 y ss.
- 36 - Vid. Del Vecchio,: "*Filosofía del Derecho*". Ed. española, 1929, pág.219.
- 37 - Vid. De Castro y Bravo, F.: "*Derecho Civil de España*". Madrid, Cívitas, 2ª ed. y *"Temas de Derecho Civil"*. Marisal, Madrid, 1972.
- 38 Así Lehman y la teoría de los "property raigth" que hoy se aplica a la propiedad intelectual e industrial.

cuanto medio coercitivo de hacer valer en juicio la facultad correspondiente ("derecho subjetivo es el que va acompañado de una acción para la realización de las consecuencias jurídicas en caso de violación"), también ha entrado en crisis pues hay derechos y obligaciones que carecen de ella. Como consecuencia de ello se sustituye el concepto de acción por otro mas amplio: *la garantía jurídica* en la que caben distintos medios de protección, como dice Castán, "y que tiene la ventaja de no excluir de la categoría de derechos de los que dimanan de las llamadas obligaciones naturales". Este mismo autor, señala cuáles son los **elementos** que integran el derecho subjetivo: *la voluntad apta del sujeto*, que forma el "substrato del derecho", *la facultad o poder jurídico*, reconocida al titular e integrada por una o varias facultades unidad en un haz o conjunto, sería el "elemento sustancial o contenido" del derecho. Tal contenido tiene dos aspectos: la posibilidad de exigir un comportamiento y la posibilidad de obrar válidamente, y coinciden con el elemento externo e interno antes comentados. El *elemento normativo* representado por el ordenamiento que sanciona y protege ese derecho. El *interés* jurídicamente protegido por ese derecho, que puede ser moral, personal o puramente material o económico. Por último, *los medios coactivos de defensa*, integrados por las garantías jurídicas puestas al servicio del titular y su derecho, así la acción, excepción, autodefensa, etc... [39] Gullón y Diez Picazo ponen de manifiesto que la idea de derecho subjetivo "implicaba un problema de organización social", pues supone dotar al titular de un ámbito independiente de actuación, lo cual conecta el concepto con la libertad y dignidad, valores fundamentales de la persona, por ello afirman: *"apostar por el derecho subjetivo es apostar por la libertad"*, frente al intervencionismo estatal, frente al desmesurado crecimiento de los medios técnicos de intromisión en la esfera de libertad y en la privacidad del sujeto, nos encontramos con la figura del derecho subjetivo como ámbito de libre actuación de la persona, como instrumento de su libertad y de su dignidad, por ello dicen: "En cambio, *la libertad tiende a ser máxima en el desarrollo de la personalidad*, y de ahí la acusada proliferación de los derechos humanos en sus múltiples facetas".[40] Estas palabras cobran especial significado cuando estamos ante derechos subjetivos cuyo objeto esta integrado por bienes pertenecientes a la esfera personal o moral del titular, pues en tales casos la conexión derecho-libertad-dignidad está muy acentuada. Cuando estamos ante los llamados *bienes esenciales* nos referimos a aquellos que atañen a la existencia física o jurídica de la persona, como afirmaba De Castro, en cuanto son imprescindibles para una digna existencia del sujeto. La vida, la integridad, la libertad, el honor o la intimidad son bienes

- 39 - Vid. Castan Tobeñas, J.: *"Derecho Civil Español Común y Foral"* Revisada y puesta al día por De los Mozos, J.L.; Reus, Madrid, 14ª ed., Tomo I, vol.2º.
- 40 - Vid. Gullón Ballesteros, A. y Diez Picazo, L.: *"Sistema de Derecho Civil"*. Técnos, Madrid, 7ª ed., vol.1, pág.433 y ss; igualmente LASARTE en op.cit.

que el sujeto debe tener protegidos por cuanto ello atañe directamente a sus condiciones de existencia, ya sea como individuo (vida) o en cuanto miembro de la comunidad (honor). En función de ello se ha hablado de *bienes individuales y sociales de la persona.*[41]

En base a ello, nos encontramos con unos derechos subjetivos cuyo objeto es extrapatrimonial, referido a elementos o condiciones del titular en cuanto persona, por lo que se adquieren de forma originaria, son esenciales e inherentes a su condición, absolutos, en cuanto exigibles frente a todos, intransmisibles, irrenunciables e imprescriptibles. A partir de esa conexión derecho subjetivo-persona-libertad se puede afirmar que ciertos derechos subjetivos, antes citados, por su condición de inherentes a la persona se conforman como el instrumento adecuado para garantizar al individuo una esfera de actuación para el desarrollo de su personalidad, libre de intromisiones o coacciones externas por parte del Estado o los otros miembros de la comunidad. En tal caso, estamos ante derechos básicos que debe poseer toda persona dentro del marco de un Estado de Derecho, de ahí que se les denomine como *derechos fundamentales de la persona* y en los ordenamientos modernos posean una consagración y tutela de índole constitucional. No obstante, hay que decir que el concepto de derechos fundamentales es moderno pues viene ligado al desarrollo del Estado Moderno. La ideología liberal los conceptúa como una esfera de inmunidad frente al Estado que se consagra en la Declaración de los Derechos del Hombre, basada en una óptica iusnaturalista. Pero tales declaraciones son fundamentalmente programáticas, actúan como principios o valores carentes de una eficacia y fuerza de obligar ya que no se incorporan al Derecho positivo ("Los derechos se **pueden**, no se tienen"). Es preciso pues dar el siguiente paso: incorporarlos a la norma positiva para que puedan realmente desplegar su eficacia y fuerza protectora del sujeto, superándose así el estadio anterior de simples valores programáticos. En esta nueva situación cabe ya entenderlos, según Peces Barba, como "facultad que la norma atribuye de protección a la persona en lo referente a su vida, a su libertad, a la igualdad, a su participación política o social, o **a cualquier otro aspecto fundamental que afecte a su desarrollo integral como persona**, en una comunidad de hombres libres, exigiendo el respeto de los demás hombres, de los grupos sociales y del Estado y **con posibilidad de poner en marcha el aparato coactivo del Estado en caso de infracción**". [42] Por tanto, la consagración de tales derechos en los textos constitucionales es definitoria del modelo social que se implanta, pues constituyen la llamada *"parte dogmática"* de las Constituciones que informa el conte-

■ 41 - Vid. De Castro: "Temas..." cit. loc. cit.

■ 42 - Vid.PECES BARBA, G.: *"Derechos Fundamentales"*. Madrid, 1976; en lo referente a esta materia nos remitimos a la excelente obra de PEREZ LUÑO, A.E.: *"Derechos Humanos, Estado de Derecho y Constitución"*. Técnos, Madrid, 3ª edición, ya que con ella puede obtenerse un completo e interesante conocimiento de la materia.

nido valorativo del orden constitucional. Por otra parte, frente a la actitud absentista del Estado liberal, el Estado democrático de Derecho ha de adoptar una actitud de *promoción y posibilitación* de tales derechos, evitando los obstáculos y condicionamientos para el ejercicio y tutela de tales derechos; el Estado viene vinculado por tales derechos, siendo uno de los principios rectores de la política de actuación la promoción y defensa de los mismos. Se ha señalado por la doctrina [43] que nuestra Constitución hace una auténtica declaración de derechos pues el contenido de su Capitulo 2°, del Titulo I, "es una concreción del enunciado de valores que expresa en el artículo 1.1". Es decir, que esos *valores superiores* se concretan posteriormente en el texto constitucional, incorporándolos al Derecho positivo y superando su mera condición programática. Partiendo de un núcleo-valor esencial: libertad e igualdad, se van concretando en toda una serie de derechos y libertades que se constituyen en la base del orden político y la paz social (Cfr. arts 9.2 y 10.1 C.E.). Ese carácter nuclear hace que los derechos fundamentales se caractericen como un componente del **orden público** pues son *"un núcleo indispensable para la convivencia"* (Suárez Pertierra).

La regulación de la materia en nuestra Constitución es moderna y está influida por textos coetáneos como la Constitución Portuguesa, incorporando derechos de nuevo cuño, como medio ambiente, y utilizando un criterio interpretativo flexible que supone la admisión de que los derechos fundamentales son una categoría abierta en la medida en que incorporan los valores esenciales de la comunidad, transcendiendo de su aspecto meramente individual, lo que se pone de manifiesto en las modernas teorías sobre la legitimación para su ejercicio. En este sentido ha de entenderse la remisión a la Declaración Universal de los Derechos Humanos y los Tratados y Acuerdos ratificados por España sobre tales materias. (art. 10.2 C.E.), pues se trata de una norma que permite adaptar y "poner al día" a nuestro ordenamiento en atención a la evolución social. El criterio sistematizador que ha seguido la Constitución se basa en la protección que cada uno de ellos recibe: Los derechos que vienen recogidos en el artículo 14 y en la Sección 1ª del capítulo II, son protegidos a través de un procedimiento basado en los principios de preferencia y sumariedad (art. 53.2 C.E.) y, en su caso, del recurso de amparo ante el Tribunal Constitucional (cfr. art. 43 y D. Tr. 2ª L.O.T.C.). Los derechos ciudadanos incluidos en la Sección 2ª están protegidos por el recurso de inconstitucionalidad del artículo 161.1 C.E. Se trata de una gradación atenta a la mayor o menor fuerza de protección que se dispensa a tales derechos; la primera Sección tiene una protección reforzada ya que está referida a derechos atribuidos a *todos* por lo que las garantías protectoras han de ser las más eficaces porque con ello se corres-

■ 43 - Vid. Suárez Pertierra, G.: "*Comentario introductorio al Capitulo II C.E.*". En "Comentarios..." EDERSA, cit. pág. 268.

ponde con la función que tales derechos cumplen en un Estado social y de Derecho.[44]

No obstante, la doctrina ha planteado la dificultad de aplicar el concepto y estructura del derecho subjetivo a los derechos de la personalidad, así De Castro al abordar la cuestión distingue unos *bienes esenciales, vida, integridad personal, libertad,* de otros de carácter *social,* que están referidos a realidades externas de la persona, los cuáles poseen una cierta independencia que les acerca a las notas del derecho subjetivo.[45] Frente a ello, autorizadas opiniones consideran que el derecho subjetivo es un concepto técnico jurídico extraído del campo patrimonial lo cual ha hecho que se dificulte su aplicación a figuras más recientes como los derechos de la personalidad. Ese desajuste entre el concepto previo y la categoría posterior no es razón para negar la aplicación del derecho subjetivo como instrumento de técnica jurídica destinado a proteger a la persona y sus bienes materiales e inmateriales. En base a ello se afirma: "Por ello juzgamos acertada la adopción de la técnica jurídica del derecho subjetivo para la protección de la intimidad de las personas, superando la angosta vía, hasta ahora ofrecida, del artículo 1902 del Código civil, distinguiéndose esa doble proyección en que se ofrece la intimidad de los seres humanos, en sí mismos considerados, y en sus relaciones con los demás, es decir, como personas, e insertos en el grupo familiar, núcleo entrañable de la vida privada".[46] El Tribunal Constitucional se ha definido ya en el mismo sentido, pues entiende que todo derecho subjetivo cumple una función social dentro del orden de la comunidad, así la propiedad del artículo 33 C.E., nota que se acentúa en estos derechos que constituyen "el fundamento mismo del orden político-jurídico del Estado en su conjunto". Esto se deduce de su "*doble carácter*", pues en primer lugar, *son derechos subjetivos,* derechos de los individuos no sólo en cuanto derechos de los ciudadanos en sentido estricto, sino en cuanto *garantizan un status jurídico o la libertad en un ámbito de la existencia.* Por otra parte, y al propio tiempo, entiende el Alto Tribunal que son elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como un marco de convivencia humana justa y pacífica. Esta doble naturaleza se consagra tanto en la Constitución como en los Textos Internacionales y Convenios sobre la materia, como los anteriormente citados.(Cfr. STC 14 de Julio de 1981, entre otras).

Desde esta perspectiva, hemos de abordar la configuración jurídica de los derechos que la LORTAD consagra como auténticos derechos subjetivos que vienen a funcionar como *garantías* de un elemento esencial de la persona: **la**

- 44 - Vid. Suárez Pertierra op.cit.
- 45 - Vid. De Castro y Bravo, F.: "*Los llamados derechos de la personalidad*" A.D.C. 1952, pág.1263 y ss.
- 46 - Vid. Vidal Martínez, J.: "*El derecho a ...*" cit. pág.48 y ss.

libre esfera de autodeterminación sobre su privacidad, entendida ésta en el sentido antes apuntado, es decir, como bien personal de doble vertiente, íntima y externa, vinculado y tutelado por el derecho fundamental a la intimidad recogido en la Constitución en su artículo 18.1 y por esa esfera de libertad que le permite decidir sobre qué aspectos de su vida y entorno han de ser conocidos por los demás cuando pertenezcan al ámbito de los datos personales sensibles cuyo conocimiento no esté afecto al interés general o a la protección de otros bienes esenciales jurídicamente protegidos, del artículo 18.4. El titular de estos derechos es la persona física, con las precisiones arriba enunciadas, afectada por el proceso de automatización de datos. Tales derechos se confieren para la defensa de su titular frente a intromisiones o abusos cometidos por medio de la informática: recogida de datos, almacenamiento, transmisión de los mismos e incluso actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o de su personalidad, la llamada "identidad informática". El problema que la norma quiere abordar no es la existencia de bases y ficheros informatizados, sino su descontrol, el desconocimiento de su existencia, los contenidos de los mismos y su utilización ilícita o perjudicial para las personas. Por ello se crea el Registro General de Protección de Datos, dentro de la Agencia de Protección de Datos, en el cual se han de inscribir todos los ficheros de titularidad pública y privada a fin de posibilitar el conocimiento de su existencia y su control por los órganos competentes, así como para que los sujetos puedan ejercitar sus derechos frente a ellos. Por tanto, un fichero o base no autorizado e inscrito es, por sí mismo, ilegal y su titular esta en una situación de ilicitud, pues al ser oculto no se puede controlar a los efectos que la Ley pretende.

Haremos seguidamente un estudio de cada uno de estos derechos tal y como vienen recogidos por la Ley, si bien la dificultad y contenido del mismo exceden con mucho a las posibilidades del presente trabajo; pretendemos iniciar o apuntar su estudio desde una óptica omnicomprensiva integrándolos en un sistema armonizado construido al servicio de ese derecho fundamental de la persona al que antes aludiamos.

1º La Ley parte de un derecho a la ***"autodeterminación informática"***, que se inspira en el principio de que ha de ser el sujeto quien decida qué datos pueden ser almacenados, por quién y para qué fines, lo cual comporta una capacidad de decisión que descansa en una información previa o en el requerimiento inicial de su consentimiento para recabar, tratar o ceder los datos sensibles a él referentes. Estamos pues ante el "Habeas data" en virtud del cual la persona tiene la facultad de controlar la información que le concierne y que se

encuentra recogida en el fichero automatizado; le asegura una esfera de libre decisión con respeto a una categoría de datos sobre los cuales el Ordenamiento le confiere la facultad de prestar su consentimiento para ser objeto de tratamiento automatizado. Así hemos de entender el artículo 6 de la Ley cuando taxativamente dice:"el tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa"; este consentimiento, libre y consciente, formado sobre una base cierta, puede ser revocado cuando concurra una causa justificada para ello y no se le atribuya efectos retroactivos. Por tanto, el error, la mala fé o el dolor, son vicios del consentimiento que justificarían la revocación de ese consentimiento, así como la concurrencia de una nueva circunstancia que legitime al concedente para revocar aquel consentimiento prestado en circunstancias distintas, como puede ser cambio de empresa o de estado civil, etc...

Este consentimiento tampoco se ha de recabar cuando se recojan los datos de fuentes accesibles al público, así una biografía autorizada, o cuando se recojan para el ejercicio propio de las funciones de las Administraciones públicas en el ámbito de sus competencias, o cuando se trate de personas inmersas en el seno de una relación negocial, laboral, administrativa o un contrato **y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato**. Este párrafo del artículo 6.2 además de reiterativo, implica que sólo los datos **pertinentes** o adecuados para la relación de que se trate pueden ser objeto de tratamiento sin consentimiento del afectado, pero obviamente, cuando ya no sean necesarios o pertinentes, deberán ser cancelados, en cumplimiento del antes mencionado derecho al **olvido**.[47]

Este derecho constituye, por tanto, como dice Pérez Luño "un cauce procesal para salvaguardar la libertad de la persona en la esfera informática, que cumple una función paralela, en el seno de los derechos humanos de la tercera generación, a la que en la primera generación correspondió al "habeas corpus" respecto de la libertad física o de movimientos de la persona". [48] Con ello se constituye como una auténtica garantía plenamente eficaz para la protección de la esfera de libertad de la persona frente a los abusos cometidos por medio de los instrumentos informáticos. Como consecuencia de ello, deben ponerse al servicio de este derecho todo un conjunto instrumental de garantías jurídicas, cristalizadas en derechos subjetivos, que actúan en defensa del mismo, bien mediante información previa que posibilite la formación de un consentimiento libre y cierto, o por el conocimiento posterior y sus consecuencias en orden a la

■ 47 - Recordemos aquí los conocidos "test" tan utilizados en la selección de personal o en las pruebas para el ingreso en la IMEC cuyo contenido, en muchos casos, está formado por datos "supersensibles" como afiliación política, vida y "fantasías sexuales", tendencias y manías personales, etc... y cuya finalidad y situación actual es bastante "oscura".

■ 48 Vid."Intimidad y protección...". cit. pág. 40.

rectificación o cancelación de los datos. En definitiva, toda recogida y tratamiento de datos personales sensibles, así como su cesión, han de contar con un consentimiento expreso o una habilitación legal, pues de lo contrario es ilícito y, por tanto, ha de cancelarse (cfr. art. 6 y 11). Téngase en cuenta que en el artículo 4.7 se consagra un principio fundamental por el que se **prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos**, por lo que todo dato adquirido por tal medio es contrario a la norma siendo nulos los efectos que pueda operar y genera la responsabilidad, civil y penal, correspondiente.

2º *El derecho de Información.*

Este derecho, que posee una doble vertiente, está consagrado en los artículos 5 y 13 (expresamente en éste) de la Ley en virtud de los cuales los sujetos a los que se recaba datos personales, dentro del respeto a su derecho de autodeterminación, han de ser informados de forma *expresa, precisa e inequívoca* de los siguientes extremos:

a) de la existencia, finalidad y destinatarios de la información que se solicita.

b) del carácter obligatorio o facultativo de su respuesta a la solicitud y de las consecuencias de la recogida o negativa a suministrarlos.

c) de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

d) de la identidad y dirección del responsable del fichero.

Cuando se utilicen cuestionarios o impresos tales advertencias han de figurar de forma legible y clara en los mismos. No obstante, estas advertencias no se precisan si de su contenido se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que estos datos se recaban.

Este derecho se convierte en el escalón inicial a partir del cual se posibilita el ejercicio de los otros derechos recogidos en el Título III pues es necesario que el sujeto conozca la existencia del fichero, su contenido, su finalidad y su titular, así como los derechos que le asisten y si tal información puede o no ser recogida y tratada pese a su negativa a facilitarla.

En cuanto a los ficheros de titularidad privada se impone la obligación de comunicar la información cuando sean datos sobre los cuales no se haya pedi-

do el consentimiento del afectado, como sucede en el artículo 28.2 con los datos relativos al cumplimiento de las obligaciones dinerarias, tales tipos de datos solo pueden estar referidos, cuando sean adversos, a un máximo de 6 años.

Por otra parte, la obligación de inscribir los ficheros en un Registro General de Protección de Datos, creado al efecto, tal y como impone el artículo 38, supone el dotar de un extraordinario instrumento de conocimiento para este derecho de información que comentamos, a la vez que medio imprescindible para el ejercicio de los otros derechos reconocidos en la norma, de tal suerte que todo fichero que incumpla los dictados de este precepto es ilegal, con las consecuencias a ello inherentes. Es por ello que el artículo 13 faculta a *cualquier persona* para consultar, pública y gratuítamente, Registro a fin de conocer la existencia de ficheros automatizados de datos personales, de sus finalidades y de la identidad del responsable del mismo, como base y fundamento para el ejercicio de los derechos que le asisten. Así se conceptúa el Registro en el artículo 23 del R.D. 428/93 de 26 de Marzo, que aprueba el estatuto de la Agencia de Protección de Datos, a cuyo tenor éste es un Organo de la Agencia al que "corresponde velar por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal **con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación**".

El artículo 22.1 contiene una excepción a lo dispuesto en el artículo 5.1.2 cuando la información impida o "dificulte" gravemente el cumplimiento de las funciones de control y verificación de la Administraciones públicas, o afecte a la defensa nacional, a la Seguridad pública o a la persecución de infracciones penales o administrativas. Esta es una de las excepciones por "razón de Estado" que protegen el "oscurantismo" estatal que puede dar pie a abusos incontables y se nos antoja de bastante dudosa admisibilidad.

3º- *Los derechos al* ***Silencio y al Olvido.***

Formulados por la doctrina más reciente, antes citada, podrían considerarse implícitos en el espíritu de la Ley, en concreto en el artículo 10 que impone el deber de mantener el secreto sobre tales datos a las personas que intervengan en cualquier fase del tratamiento de los mismos. Dicha obligación se mantiene incluso cuando cese la relación del obligado con el titular o responsable del fichero. Esto es consecuencia del deber de buena fe contractual de honda raigambre en nuestro sistema jurídico y como consecuencia del estatuto funcionarial en los empleados públicos. El artículo 4.5 consagra un principio de protección de datos que genera un deber inexcusable de cancelar de oficio los datos personales cuando dejen de ser necesarios o pertinentes para la fina-

lidad con la que se recabaron y registraron, independientemente de que el sujeto afectado lo solicite. Igualmente, en el artículo 20.4 se impone el mandato de que los datos personales registrados con fines policiales sean cancelado de oficio cuando dejen de ser necesarios para las averiguaciones que motivaron su almacenamiento. En el artículo 27.2 se impone la misma obligación en el seno de las relaciones privadas de prestación de servicios (así médico o abogado) pues una vez cumplida la prestación deben cancelarse los datos ("destruidos") recabados en razón de la misma, salvo consentimiento expreso de la persona por cuenta de quién se prestó el servicio, porque razonablemente se presuman nuevos encargos, en cuyo caso se han de almacenar con la debida seguridad. De estos preceptos podemos decidir, implícitamente, lo que se ha dado en llamar el "derecho al olvido".

Se trata por tanto de la situación en que la existencia y contenido de los datos debe quedar dentro del ámbito funcional y finalidad del fichero para el que fueron recabados evitando el "rumor" informático (Dº al silencio) y del derecho a que, de oficio, el titular o responsable cancele o destruya los datos personales cuando se dén alguno de los supuestos antes citados, sin que tenga que mediar previamente el ejercicio del derecho de cancelación (Dº al olvido). Panuccio lo define gráficamente como el derecho a eliminar el dato personal de la memoria colectiva, cancelando aquellos datos que han perdido el contenido de interés, actualidad u oportunidad, en este sentido sería un derecho a la cancelación de oficio, si bien ésta es un medio para la realización de aquél. Repetimos que ambos derechos no figuran expresamente recogidos en la ley pero se deducen del contenido de deberes jurídicos que la norma impone a los titulares de los ficheros, y como reverso de tal deber los consideramos derechos por cuanto tal conducta puede ser exigida coactivamente por sujeto afectado; en razón de ello la doctrina no duda en considerar que estamos ante un verdadero derecho subjetivo. [49]

En lo relativo a los derechos expresamente consagrados, al margen del citado derecho de Información, en el Título III queda patente su carácter instrumental y de dependencia con respecto al derecho a la libre autodeterminación antes citado, por cuanto actúan como instrumentos para la plena satisfacción del interés múltiple protegido por el mismo.

4º- *Derecho de* ***Impugnación.***

Ya hemos aludido a la "diabólica combinación de las palabras" y al "rumor informático" frente al cual se erige el derecho al silencio; junto a ello

■ 49 - Vid. Panuccio, V.: "Banche dati...". cit. pág.81 ss.

tenemos el riesgo que comporta la confección de la llamada "identidad informática" tal y como la misma Ley teme cuando dice: "Los mas diversos datos -sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado dinero de plástico, sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideologías, por poner sólo algunos ejemplos- relativos a las personas podrían ser así compilados y obtenidos sin dificultad". Todo ese cúmulo de información puede ser tratada de forma que entrañe un peligro para el sujeto afectado pues "ello permitiría a quién dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo debe tener acceso el individuo y, quizás, quienes le son más próximos, o aquéllos a los que él autorice". Esta posibilidad entraña un peligro real que no escapa al Legislador: "el conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; **y este perfil, sin duda, puede resultar luego valorado *favorable o desfavorablemente*, para las más diversas actividades públicas o privadas**, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos". Este perfil o identidad informáticamente obtenidos es en sí mismo una finalidad prohibida por la Ley, tal y como cabe deducir de los dictados del artículo 7.4, y las decisiones basadas en tal "perfil" son impugnables como el artículo 12 dice expresamente: "El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo *único fundamento* sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad". Este derecho así enunciado es positivo, pero el problema es que pocas resoluciones son fundadas, y menos en la actividad privada, sino que se "disfrazan" junto a otras pruebas poco relevantes pero que permitirían enervar la impugnación dado que ya no estaríamos ante el "único fundamento". No obstante, supone el freno a prácticas que la Administración y las empresas han venido realizando de forma reiterada.

- 5º- *El derecho de* ***Acceso***.

Deducido del derecho de información, es el eje del sistema de garantías arbitrado por la norma que lo consagra en el artículo 14, y faculta a su titular para exigir el conocimiento preciso de los datos de carácter personal relativos a su persona que se incluyan en un fichero automatizado, se trata del derecho a controlar el contenido de los ficheros automatizados relativo a la esfera personal del titular. El contenido de la información que se le facilite ha de ser completo y exacto, salvo las excepciones que la norma consagra para ciertos

temas tales como defensa, seguridad o hacienda; la consulta puede consistir en una visualización del contenido o bien puede exigirse la entrega de un documento fehaciente de dicho contenido, sea escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin que se utilicen claves o códigos que precisen el uso de dispositivos mecánicos específicos; lo recomendable es, desde luego, pedir copia por escrito y certificada pues es el medio más seguro de poder disponer de una prueba en caso necesario. De la lectura del artículo 16.2 se deduce la gratuidad de la rectificación y cancelación, pero no así del ejercicio del derecho de acceso, extremo éste que se deberá fijar en la futura reglamentación del procedimiento que el legislador promete. Este derecho se puede ejercitar en plazos no inferiores a de 12 meses, excepto cuando concurra un interés legítimo al efecto, que faculta para ejercitarlo antes, lo cual no es muy de recibo dada la naturaleza de la cuestión y el hecho de que, seguramente, se deberá pagar una contraprestación por su ejercicio. Su ejercicio no procede cuando concurran ciertas excepciones previstas para casos en que la ley así lo establezca, siendo éste uno de los aspectos más criticados de la misma antes y después de su aprobación, y que se consagran en los artículos 21 y 22, básicamente, para ficheros de titularidad pública, los únicos para los que la Constitución consagra expresamente este derecho en su artículo 105.b al cual se le imponen más excepciones. Fundamentalmente, las excepciones obedecen a razones de seguridad y se refieren a ficheros de las fuerzas de seguridad del Estado, artículos 20.2.3.4 y 21.1, pues se faculta a sus responsables a denegar el ejercicio de este derecho, y sus consecuentes, cuando de ello se deduzca riesgo para la defensa, la seguridad, los derechos de terceros o las necesidades de las investigaciones en curso. Lo mismo pueden hacer los responsables de los ficheros de la Hacienda pública cuando esta en curso un procedimiento inspector o se obstaculicen las labores tendentes a asegurar el cumplimiento de las obligaciones tributarias. En estos casos no se prevé una resolución motivada, como sí sucede cuando la negativa obedece a que tales derechos han de ceder ante razones de interés público o ante intereses de terceros más dignos de protección; en cuyo caso el órgano administrativo dicta resolución motivada e instruye al afectado de su derecho a acudir a los órganos pertinentes. (art.22.2)

Frente a ello la ley faculta al afectado a dirigirse a la Agencia de Protección de datos, u organismo competente en la Comunidad Autónoma, "quién deberá asegurarse de la procedencia o improcedencia de la denegación"; este cauce nos parece previo pero el afectado, a nuestro juicio, acabará acudiendo a los Tribunales de Justicia último recurso frente a la discreccionalidad que la norma permite a los órganos de la Administración para denegar el ejercicio de un derecho-garantía al servicio de un derecho fundamental, si bien la legislación administrativa impone resolución motivada en el caso de ficheros de titu-

laridad pública. Estas excepciones son de dudosa constitucionalidad pues vulneran la presunción de inocencia, la tutela judicial efectiva, el derecho a ser informado de los cargos y procedimientos, y lo que es más grave, impide el lógico ejercicio de los derechos de rectificación y cancelación, con lo que el sujeto no sabe qué se le investiga, porqué y para qué, en base a qué datos y, sobre todo, puede ser sancionado, o algo peor, en base a datos que pueden ser incorrectos o inexactos o deben estar ya cancelados, pero nada de ello puede impedir porqué no tiene posibilidad de acceder a la información que se utiliza contra él!

Por otra parte, el derecho de acceso a los archivos y registros públicos que consagra el artículo 105.b de la Constitución está recogido como uno de los "derechos de los ciudadanos" en el artículo 37 de la la reciente Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Civil Común (Ley 30/92 de 26 de Noviembre) incluyendo los derechos de rectificación y cancelación cuando sean datos que afecten a la intimidad de la persona, o formen parte de un expediente ya caducado; no obstante el 37.4 permite denegar el acceso cuando ello obedezca a razones de interés público o intereses de terceros más dignos de protección o lo disponga una Ley, si bien en tales casos debe dictarse resolución motivada. El párrafo 5º enumera toda una serie de expedientes respecto a los cuales no puede ejercitarse este derecho: investigación de delitos, defensa nacional, actuaciones del Gobierno, etc... otros se han de regir por disposiciones específicas: expedientes sanitarios, materias clasificadas, etc...

Por todo ello, el derecho de acceso cobra plena virtualidad en el campo de los ficheros de titularidad privada, pues las limitaciones y excepciones que a éste y los otros derechos derivados de él les imponen las Leyes hacen bastante difícil entender a qué ficheros y datos de su interés podrá acceder el afectado.

6º- *Los derechos de* ***Rectificación y Cancelación.***

Si como consecuencia del ejercicio de este derecho, el titular constata que los datos contenidos en el fichero son inexactos, incompletos o han dejado de ser pertinentes o adecuados en atención a la finalidad para la que se registraron, puede *exigir* bien su rectificación, o que se completen, en ejercicio de su **derecho de rectificación**. Por otra parte, si tales datos no son pertinentes o adecuados en base a aquella finalidad o relación que originó su registro, o pertenecen a la esfera privada del sujeto en tal grado que éste no desea que se registren, y no viene obligado a permitirlo fuera de los supuestos que la norma establece, podra ejercitar su **derecho de cancelación o de bloqueo** exigiendo

que se borren o bloqueen tales datos, es decir que desaparezcan del fichero o queden imposibilitados de uso o trasmisión desde el mismo, el procedimiento para el ejercicio de estos derechos queda también a una futura regulación, pero si afirma la Ley su gratuidad, siendo ello lógico por cuanto la causa le es imputable al titular del fichero. Como consecuencia de lo anterior, si los datos rectificados o cancelados han sido previamente cedidos, dichas circunstancias serán comunicadas por el responsable del fichero al cesionario para que obre en consecuencia. Así mismo, todo dato personal inexacto o incompleto ha de ser cancelado una vez rectificado, ya que esta circunstancia hace innecesario su mantenimiento. Sin embargo, la norma contiene unas limitaciones a tales derechos, siendo unas más admisibles que otras, sobre todo las que se refieren a ciertos ficheros de titularidad pública como los de policía, defensa o hacienda pública, tal y como consagra el artículo 21, siendo ésta la parte más criticable de la Ley. El derecho de cancelación tiene previstas otras limitaciones en el artículo 15, la primera de ellas tiende a impedir que la cancelación perjudique *intereses legítimos de del afectado o de terceros* o porque exista obligación de conservar los datos. Vemos difícil que un tercero o "afectado" tenga interés legitimo en que se conserve un dato personal ajeno, y el propio afectado es quien insta la cancelación sabiendo las consecuencias de ello; el tercero puede ser la Administración, que ya se encarga de asegurarse la mayor discreccionalidad para decidir y limitar estos derechos. Por otra parte, tampoco procede cancelar los datos antes del plazo legalmente establecido para ello en las disposiciones aplicables (¿así los cinco años de Hacienda?) o, en su caso, el plazo previsto en la relación contractual entre el *afectado* y el responsable del fichero, si bien éste ha de cancelarlos de oficio una vez transcurrido el plazo o extinta la relación contractual, tal y como le exige el artículo 27.2.

El fundamento de estos derechos reside en ese derecho de autodeterminación ya comentado, si bien el principio de "calidad de los datos" del artículo 4 impone que tales datos sean adecuados, pertinentes y no excesivos en relación con las finalidades y ámbito para el que se recogen, lo cual implica que la rectificación y cancelación se puede exigir cuando el dato es excesivo, no pertinente o inadecuado, no sólo cuando es inexacto. En el art. 4 se imponen unas obligaciones de conducta de oficio al titular del fichero: mantener los datos exactos y al día, rectificándolos de oficio, sustituyéndolos por los correspondientes datos rectificados y completos, sin que sea necesario que ello se solicite. Los datos deben cancelarse de oficio cuando ya no sean pertinentes o necesarios para la finalidad con que se recogieron, mientras tanto, deben estar almacenados de forma que posibiliten el ejercicio de los derechos de los afectados. El incumplimiento de estos deberes supone negligencia por parte de las personas encargadas del fichero y, por tanto, el incurrir en responsabilidad por tal conducta.

En definitiva este **derecho a la autodeterminación informática** se concreta en unos derechos subjetivos de carácter personal, esencial, indisponible e imprescriptible que se predican de la persona en cuanto tal, y que están concebidos por el Legislador como garantías jurídicas al servicio del derecho fundamental a la privacidad frente al uso de los medios informáticos, lo cual les asimila por su propia naturaleza y función a los llamados "derechos fundamentales de la tercera generación", si bien tienen un carácter instrumental con respecto al derecho constitucional a la intimidad del artículo 18, que se concreta en la privacidad como nuevo contenido "globalizador", tal y como vimos anteriormente. Por otra parte, existen unos derechos no consagrados formalmente como tales en cuanto surgen por la vía de figurar en la Ley como "deberes imperativos de conducta" que recaen sobre los titulares de los ficheros automatizados que vienen compelidos a una conducta profesional diligente marcada por los llamados "principios de protección de datos", plasmados en el artículo 4 y vertebrados en otros, que plantean unas exigencias de calidad de los datos objeto de tratamiento: licitud, oportunidad, adecuación, pertinencia, veracidad y exactitud; el "reverso" de este "deber legal" es un derecho-acción que asiste al sujeto afectado para reclamar frente al incumplimiento de tales deberes. De salida, la norma en su Título Segundo *"Principios de la protección de datos"* dicta unos mandatos imperativos, a la vez que principios rectores, a los que habrán de atenerse los titulares de los ficheros.[50] En base a ello, cabe entender que los derechos-garantías se han de ejercitar toda vez que se incumplen estos imperativos legales, pero que no es necesario, como hemos visto, el ejercicio del derecho para que el titular del fichero venga obligado a actuar conforme a la Ley. El artículo 4.1 marca el primer límite: "Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho tratamiento cuando tales datos sean *adecuados, pertinentes* y *no excesivos*, en relación con el *ámbito y las finalidades legítimas* para las que se hayan obtenido". Tales conceptos son un tanto inconcretos, pero aplicados al contexto de la norma: la relación entre la persona y el titular del fichero y la finalidad del mismo, permiten una flexibilidad de criterio a la hora de valorar los incumplimientos.

De otro lado, el artículo 4.2 veda el uso de los datos personales objeto de tratamiento automatizado para *cualquier finalidad distinta* de aquella para la que fueron recogidos. Es decir, tales datos están recogidos para un fin determinado, así investigación médica, contrato de préstamo, tarjeta de crédito, relación laboral, etc... y no pueden utilizarse, ni transmitirse, para otra finalidad

■ 50 - Según el artículo 3.a fichero automatizado es "todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

diferente a ésta. El párrafo 5º impone que cuando los datos han dejado de ser necesarios o pertinentes para la finalidad prevista *han de ser cancelados*; ello quiere decir, que cuando se extingue la relación preexistente que motivó la recogida, el titular del fichero debe de oficio *cancelarlos.* Es también importante, el mandato de los párrafos 3 y 4 del artículo citado: los datos han de ser *puestos al día de forma que respondan con veracidad a la situación real del afectado.* Si tales datos resultan parcial o totalmente inexactos o incompletos, *serán cancelados y sustituidos* ***de oficio*** por los correspondientes datos rectificados o completados. En todo caso, el almacenamiento de los datos se ha de hacer de forma que permita el ejercicio del derecho de acceso por parte del afectado, lo cual implica la ausencia de claves secretas o archivos ocultos, pues ello es inmediatamente contrario a la norma. La seguridad interna del fichero y la obligación de secreto de las personas relacionadas con el mismo son sancionadas expresamente por la norma en los artículos 9 y 10, su incumplimiento acarrea las sanciones correspondientes, aparte de la responsabilidad frente al afectado, en estos preceptos se fundan los derechos al silencio y secreto.

El conocimiento y consentimiento del sujeto titular de los datos personales es el eje central de la norma y así lo establece como premisa básica el artículo 6: "El tratamiento automatizado de los datos de carácter personal **requerirá el consentimiento** del afectado, *salvo que la Ley disponga otra cosa*". Nos movemos dentro del campo de los datos sensibles y supersensibles que antes enunciábamos, por lo que el artículo 16 de la C.E. es un límite a esa posible excepción establecida por la Ley. Es claro que cuando se trate de datos recogidos en instrumentos de acceso al público, Registro de la Propiedad, Mercantil o guía telefónica (Confróntese el artículo 26), no será preciso el consentimiento, como establece el artículo 6.2. Ahora bien, el mismo apartado 2 excluye el consentimiento cuando "se recojan para el ejercicio de las funciones propias de las Administraciones públicas *en el ámbito de sus competencias*, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato *y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato*". Aquí no cabe margen para la discreccionalidad, por lo que hemos de aplicar dos límites: los establecidos en el artículo 4: que sean datos pertinentes, no excesivos y adecuados a la relación y finalidades legítimas del caso, y que cuando dejen de ser precisos o se extinga la relación se cancelen de oficio. En segundo lugar los límites constitucionales del artículo 16 que la ley plasma en su artículo 7 al abordar el tratamiento de los datos supersensibles:

- Nadie puede ser obligado a declarar sobre su ideología, religión o creencias, para el tratamiento de tales datos es imprescindible el consentimiento del afectado, *sin excepciones.*

- Los datos de origen racial, salud y vida sexual sólo pueden ser recogidos, tratados y transmitidos con consentimiento del afectado, salvo que prime el interés general o lo disponga una Ley. Realmente, poco interés general debe haber en el origen racial, si no es para discriminar y quebrar el principio de igualdad. En cuanto a la vida sexual... no acabamos de entender tal interés. La salud puede ser necesaria para el tratamiento del afectado, prevenir contagios y para la investigación, como dice el artículo 8, si bien el deber de seguridad y secreto es imprescindible. A nuestro juicio, por la importancia de los bienes protegidos y los serios peligros que puede ocasionar, esta posibilidad discrecional debe interpretarse con criterios muy restrictivos, ya que incluso se duda de su constitucionalidad por algún sector doctrinal. [51]Los ficheros cuya única finalidad sea contener datos supersensibles quedan prohibidos por el artículo 7.4. Por último, los datos sobre infracciones penales o administrativas sólo pueden estar en ficheros de titularidad de las Administraciones competentes.

En definitiva, los derechos subjetivos consagrados por la norma como garantía del derecho fundamental a la intimidad (en su acepción global de privacidad) forman una categoría que se complementa entre sí mismos, unos consagrados expresamente por la norma, y otros como inherentes a ese derecho globalizador a la libre determinación emanado del derecho fundamental a la privacidad, pero en todo caso, son derechos que funcionan a modo de garantías que imponen deberes de conducta a los poderes públicos y a los demás ciudadanos, a la vez facultan para accionar frente a la lesión producida a tan importantes bienes de la persona.

V. Las Condiciones para el ejercicio de estos Derechos.

Decíamos antes que "los derechos no se tienen, se pueden" y con esta gráfica frase nos referíamos al hecho de que el problema básico no es tanto el reconocimiento legal de un derecho, cuanto dispone de los cauces adecuados para hacerlo valer. Ciertamente, un derecho desprovisto de acción está falto de un elemento esencial: la posibilidad de obtener el cumplimiento de la conducta debida por carecer del mecanismo coercitivo necesario para imponer el deber que todo derecho conlleva.

El Ordenamiento pretende asegurar al titular del derecho una esfera de libertad exenta de intromisiones ilegitimas, lo cual comporta la facultad exclusión y de actuación libremente decididas por el sujeto. Para ello se arbitran unos

■ 51 - Basta con visionar los cuestionarios psicológicos, vulgo "tests", que se realizan para algunas selecciones de personal y en el servicio militar, para comprender la situación. Véase el diario "El País" del miércoles, 15 de Mayo de 1991.

medios de defensa, la primera de las cuales tienen carácter preventivo evitando posibles lesiones, tal es el caso de la seguridad jurídica cautelar a la que sirven los principios de la protección de datos. Por otro lado, se arbitran unos mecanismos coercitivos para reprimir y sancionar las conductas lesivas ya realizadas, esta sería la vía administrativa y judicial. Esta segunda posibilidad contiene unos procedimientos que están en función del tipo de bien jurídico protegido por el derecho y de la lesión ocasionada. Existe finalmente una forma más "primitiva" de defensa: la autotutela, en virtud de la cual se faculta al individuo para que, en ciertas circunstancias, pueda utilizar legítimamente la coacción para salvaguardar sus intereses; tal sería el caso de la legítima defensa. Como norma general, es el estado quien debe tutelar el libre ejercicio de los derechos estableciendo los cauces y procedimientos adecuados para cada caso, adaptándolos a la importancia y necesidades del bien jurídico afectado.

Ya hemos puesto de relieve la importancia del bien jurídicamente protegido que se contiene en el derecho a la libre autodeterminación informática, en razón de ello se arbitra todo un complejo sistema de derechos y deberes tendentes a garantizar el cumplimiento de los fines que la norma persigue: la protección integral de la dignidad, libertad y privacidad de la persona y el aseguramiento del libre ejercicio de sus derechos. Para ello dispone el ordenamiento de dos vías: la seguridad jurídica antiprocesal y la sustantiva. La primera tiende a crear las condiciones adecuadas para evitar la proliferación de los procesos judiciales: el efecto de cosa juzgada, la imposición coactiva de determinadas medidas o resoluciones judiciales (embargo), la negativa a conceder acciones contra situaciones acogidas a unas garantías (prescripción o fe pública), la reducción del proceso y las presunciones probatorias y requisitos de prueba de las alegaciones. Por tanto, se trata de arbitrar vías de solución y prevención de conflictos que eviten las dilaciones y complicaciones de los procesos judiciales, dejando éstos como última solución.

Hasta la aprobación de la LORTAD la defensa del derecho consagrado en el artículo 18.4 se podía acoger al carácter de norma de aplicación directa que posee la Constitución y valerse de lo dispuesto en la Disposición transitoria 1ª de la L.O. 1/82 de 5 de Mayo; pero este cauce queda ahora vedado por la Disposición derogatoria única de la LORTAD, sin que ésta establezca el cauce reglamentario que permita ejercitar acciones en defensa de los derechos que ella contiene. Formulas vagas como las del artículo 15.1 y 16.1 que remiten a futuras reglamentaciones, se repiten en el artículo 17 donde se establece la posibilidad de reclamar contra las lesiones a tales derechos a la Agencia de Protección de Datos "en la forma que reglamentariamente se determine"; contra la resolución de ésta cabe recurso contencioso administrativo. En caso de ficheros de titularidad privada, la acción se ejercitará ante la jurisdicción ordi-

naria. El régimen de responsabilidad se distingue en función de si el fichero es de titularidad pública o privada, pero en ambos casos se reconoce el derecho a la indemnización.

El problema es serio dado que nos parece bien que la Agencia de Protección de Datos actúe como órgano de control de tales ficheros, públicos o privados, e incluso se le conceda un papel relevante en cuanto a la citada seguridad jurídica antiprocesal, pero la naturaleza de derecho fundamental del derecho que estudiamos y la importancia de las garantías que lo posibilitan aconsejan evitar la situación de "desprotección" en que ese afán reglamentista lo coloca. Es por ello que un sector doctrinal tachó de inconstitucional a la LORTAD por derogar la disposición antes citada de la L.O. de 1/82 sin establecer un cauce adecuado y acorde con el rango de este derecho, así se considera aún aplicable el cauce de la Ley de protección Jurisdiccional de los derechos de la persona, en base a la disposición 2ª-2 de la L.O. 2/79 de 3 de Octubre del Tribunal Constitucional. No obstante, la LORTAD remite a la Agencia y, después, a la jurisdicción competente, prometiendo la regulación reglamentaria de las condiciones de ejercicio de estos derechos, y teniendo en cuenta la importancia de los bienes implicados y el daño que los abusos pueden provocar era de esperar mayor celeridad en ese desarrollo legislativo, pues con las excepciones al ejercicio de los derechos y la falta de un sistema claro, rápido y especifico, la LORTAD crea casi más inseguridad que antes de su entrada en vigor.

De otro lado, en los ficheros de titularidad privada, el artículo 31 preve la posibilidad de acuerdos sectoriales o decisiones de empresa que tendrán el carácter de códigos deontológicos o de buena práctica profesional tendentes a regular las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad, etc... "así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas" con pleno respeto de las disposiciones de la Ley. Ello conlleva un riesgo claro: acuerdos tendentes a restringir o dificultar el ejercicio de tales derechos, por lo que deben ser inscritos en el Registro General y se podrá denegar su inscripción, y por tanto su validez, cuando se consideren contrarios a las disposiciones establecidas. Este control de la inscripción constitutiva es imprescindible para conjurar el serio peligro que esa "autonomía" normativa puede implicar en cuanto es mucho más que un mero código deontológico al poder afectar al ejercicio de los derechos de terceros.

Hemos visto pues las carencias que la Ley adolece a la hora de establecer los mecanismos necesarios para hacer efectivos los derechos que ella misma consagra y limita. Pero queremos hacer mención a otra cuestión íntimamente ligada a este tema cual es la de saber si estos derechos sólo pueden ser ejercita-

dos por el afectado en persona o si, además, cabe pensar en la existencia de terceros legitimados para ello. Se trata de derechos que protegen aspectos o valores de carácter netamente personal conectados con la dignidad, el honor, la fama o la libertad del sujeto. Tales valores, como vimos antes, conforman derechos que se ostentan en cuanto persona y en cuanto ciudadanos por lo que poseen una doble vertiente individual y social. La defensa y promoción de los derechos fundamentales es mucho más que un principio rector o programático, es un pilar fundamental de todo Estado democrático de Derecho. Desde esta óptica debemos plantearnos toda cuestión relativa a la legitimación para su ejercicio y protección.

La primera sería *¿pueden los herederos y derecho-habientes del causante ejercitar estos derechos?* Obviamente, en nuestro actual Derecho de Sucesiones está muy claro que los herederos suceden al causante en *todas las relaciones jurídicas que no se extingan a su muerte*, ello quiere decir que básicamente la sucesión opera en al campo patrimonial, pero también en todas aquellas acciones y derechos tendentes a defender valores o bienes esenciales del fallecido. En virtud de ello se faculta a los sucesores a defender los derechos de ámbito moral del autor, tal y como hace la Ley de Propiedad Intelectual, como el respeto a la autoría o a la integridad de la obra. Si ello es así con respecto a un bien considerado personal, aun cuando no constituya el núcleo de un derecho fundamental, cuánto mas será lógico afirmar que los sucesores del causante están legitimados para ejercitar los derechos consagrados en la LORTAD en defensa de la dignidad, el honor y la privacidad del fallecido.

La segunda cuestión es más complicada: ¿cabe considerar que tales derechos puedan ser ejercitados por terceros no titulares de los mismos? Hoy existen intereses o bienes de marcado carácter social que demandan protección sin que sea preciso para ello que estén atribuidos a un sujeto determinado merced a un derecho concreto. En base a ello el Derecho debe procurarles una protección aún cuando no lo demande el titular afectado, reconociendo para ello legitimación a terceros cuya relación con el bien no es de titularidad o dominio inmediato. Así, asociaciones vecinales, ecologistas y culturales defienden por vías adecuadas bienes, materiales o no, socialmente compartidos como convivencia, consumo, urbanismo, patrimonio histórico o ecología. Acciones tan antiguas como los interdictos o la acción popular, se aplican hoy a diversos campos gracias a que la "sensibilidad" de la sociedad entiende que deben ser protegidos como principios o condiciones básicas para una existencia digna.[52]

■ 52 - En este sentido cabe destacar el artículo 220 del R.D. de 28 de Noviembre de 1986 sobre Régimen de Entidades Locales, pues en caso de negligencia de éstas en el ejercicio y custodia de sus bienes y derechos, cualquier ciudadano puede exigir su ejercicio, y si la entidad no lo hiciera, "los vecinos podrán ejercitar dicha acción en nombre e interés de la entidad". Cfr. L.P. Histórico de 25 de Junio de 1985 en sus artículos 8 y 10.

Se trata de una legitimación conferida a personas físicas y jurídicas que les faculta para ejercitar acciones en defensa de unos intereses individualizados o colectivos, atribuidos o no a un sujeto determinado. Estamos por tanto ante la acción encaminada a defender los llamados "intereses difusos o colectivos", según les denomina la doctrina italiana. Así, Alpa distingue los intereses individuales, que competen al sujeto en cuanto individuo, y los intereses supraindividuales o colectivos, que le afectan y protegen en cuanto perteneciente a un grupo, colectivo o comunidad; por ello un comunero puede ejercitar acciones en defensa de la cosa común, cuanto más si se defiende un bien que trasciende a lo meramente material o económico. Tales intereses se pueden individualizar en base a un criterio subjetivo: el de que sus portadores forman componente sociológicamente individual de una colectividad, constituido en base a normas sobre organización de la pluralidad de sujetos del Ordenamiento. Por tanto, existe un interés supraindividual, colectivo, de los colectivos ciudadanos tendente a controlar el uso de la informática y sus equipos. Se trata de una "fictio iuris" que tiene por finalidad dar relevancia a todos aquellos intereses individuales que no son, o no pueden ser, accionados y, por tanto, protegidos por la inercia, indiferencia o imposibilidad del individuo. Esta suma de intereses individuales se constituye en base legitimadora de un instrumento procesal para su tutela, las modernas "class actions".[53]

El Tribunal Constitucional ha afirmado que el concepto constitucional de intereses legítimos *dispensa del requisito de que los mismos sean directos,* como exigía la L.J.C.A. en su artículo 28 o el artículo 113 del la L.P.A. que se refería a un interés directo, personal y legítimo. Nuestra Constitución no califica a los intereses tutelables de directos o personales, de lo que deduce nuestro Alto Tribunal que basta que sean indirectos, sin exigir que sean personales. Es por esta vía que la Jurisprudencia Constitucional a los intereses colectivos, y esta postura se consagra en L.O. del Poder Judicial en su artículo 7.3, a cuyo tenor: "Los Juzgados y Tribunales protegerán los derechos e intereses legítimos, **tanto individuales como colectivos**", y para accionar la defensa de estos últimos "**se reconocerá la legitimidad de las corporaciones, asociaciones y grupos que resulten afectados**". Incluso la reciente Ley 30/92 de 26 de Noviembre sobre Régimen Jurídico de las Administraciones Públicas y del Procedimiento Civil Común, en su artículo 37 dedicado al "Derecho de Acceso a los Archivos y Registros" establece en su párrafo 3º que este derecho "podrá ser ejercido, además de por sus titulares, por **terceros que acrediten un interés legitimo y directo**", sancionando con ello la afirmación que nosotros asentábamos...

■ 53 - Vid. Alpa: "*Compendio del nuevo Diritto Privatto*" UTET, Torino, 1985; Giannini: "*La tutela degli interessi colletivi nei procedimenti amministrativi*"; Rodotá: "*Le azioni civilistiche*" y López Bustos: "*La evolución de las técnicas administrativas de protección del medio ambiente*". Conferencia, Granada, 1992; A.A.V.V.: "*Group actions and consumer protection*" Bruxelles, 1992. El problema es que esta materia está mas estudiada en cuestiones tales como medio-ambiente, consumo, etc...

Esta técnica de los intereses colectivos defendidos por las llamadas "class actions" tendrá cada vez mayor desarrollo, aun cuando en la actualidad se esté circunscribiendo a temas como responsabilidad o consumo. Así, una sentencia de la Audiencia Provincial de Madrid (Sección 12) de 9 de Marzo de 1993, reconoce una "legitimación por sustitución" a un colectivo defensor de los derechos de autor sin contar con la representación del autor expresamente conferida. Todo ello nos induce a pensar que los colectivos ciudadanos, válidamente constituidos, estarán legitimados para ejercitar acciones en defensa de estos derechos reconocidos en la LORTAD en base a que defienden valores y bienes cuya protección integra uno de los intereses esenciales de la comunidad: los derechos fundamentales.

VI. Límites y Limitaciones.

Todo derecho posee unos límites y unas limitaciones, los primeros tienen su origen en el propio derecho, es decir, se derivan de su propia naturaleza y delimitan hasta dónde puede extenderse la facultad de actuación y exclusión de su titular. Las limitaciones tienen su origen en factores externos al derecho, así cabe resaltar las excepciones al ejercicio consagradas por "razón de Estado" ,de forma harto criticable, en la LORTAD. Estas excepciones han sido ya comentadas en páginas precedentes, aunque no dudamos merecen mayor tratamiento. Uno de los elementos que confluyen a delimitar los perfiles de este derecho es su relación con otros derechos, así hemos visto los límites que el derecho a la intimidad posee en relación con el derecho a la información. Hay otros derechos y principios que delimitan a los derechos que estudiamos: los que protegen intereses legítimos de terceros: así el derecho a la libre creación intelectual, el derecho de autor y la libre empresa.

En el artículo 20.1.b se consagra un derecho a crear libremente obras de carácter intelectual sin más límites que la seguridad, la defensa o los derechos de terceros. A tal efecto, la negativa a revelar datos puede obstaculizar esta creación, así una investigación médica a efectos doctorales. El artículo 30 permite sólo la utilización automatizada de los datos para tales fines cuando el afectado haya prestado libremente su autorización a tal efecto. Si ello se produce no pueden utilizarse para fines diferentes, ni cederse en forma que puedan ser relacionados con una persona concreta. Con ello se armonizan dos intereses relevantes: de un lado, el derecho del investigador a utilizar tales datos para su investigación y poder comunicarla al público, pero siempre contando con el consentimiento del afectado y, desde luego, sin darlos a conocer en forma que puedan ser relacionados con el afectado.

Por otro lado, el Ordenamiento consagra el derecho del autor sobre la obra ya creada, la llamada Propiedad Intelectual, entre cuyos objetos se encuentra los bancos o bases de datos en cuanto sistema de organización y tratamiento de la información contenida en ellos. El derecho de autor no protege la información contenida en ellos en cuanto es pública o pertenece al sujeto afectado, pero sí el soporte o sistema material creado para almacenar y tratar la información en cuanto constituye la "forma" de la obra creada por el autor, es decir, "el conjunto organizado de datos" que son objeto de tratamiento automatizado por medio de una forma de almacenamiento, organización y acceso. Se trata pues de un conjunto de datos relativos a un campo definido del conocimiento organizado de manera que puede ser ofrecido a la consulta de los usuarios, o como dice la Ley Japonesa de Dº de autor un conjunto de informaciones cuya estructura sistemática se organiza de tal manera que toda la información puede ser tratada e investigada con la ayuda de un ordenador. Con ello queda claro que no se trata de una simple compilación de información, sino que ésta debe ser estructurada de una forma sistematizada de acuerdo a un sistema o programa previo; ese "sistema organizado que estructura la información" constituye el objeto protegido por el derecho de autor, no la información recabada sea del afectado o de dominio público, así números de teléfono o sentencias o normas legales, ni el programa de ordenador que lo gestiona. Otra cuestión es que se pretenda introducir en el fichero obras protegidas por los derechos de sus autores, sin el consentimiento de éstos, en cuyo caso se estaría infringiendo el derecho de los mismos a autorizar su fijación por este medio. [54]

En cuanto a la libertad de empresa, no cabe la menor duda de que la LORTAD no supone un obstáculo a la creación de bases de datos privadas para utilizarlas en el mercado de bienes y servicios, sino que lo que la Ley pretende es establecer un sistema de control de la creación y funcionamiento de las mismas, y así se ha de entender la exigencia del informe previo del órgano de tutela y sus facultades de inspección. Se trata de evitar la indiscriminada u oculta existencia de ficheros cuyo contenido y finalidad sean contrarios a la norma, por lo que no se trata de coartar la posibilidad de crearlos, sino de regular y ordenar su existencia, contenido y fines, ello se deduce claramente del artículo 23 pues ha de ser *necesario para el logro de la actividad u objeto legítimo de la persona, empresa o entidad titular*, siempre que se respeten las garantías que la ley consagra. Con ello queda claro que un fichero relativo a datos perso-

■ 54 - Vid. Bertrand, A.: "*Le Droit d'auteur et les droits voisins*". Masson, París, 1991, pág. 432 y ss. La CEE ha elaborado una Propuesta de Directiva del Consejo relativa a la protección jurídica de las Bases de Datos, que excluye a los programas de ordenador destinados a su funcionamiento u organización, que consagra un derecho de autor a impedir las extracciones desleales. Cfr. Propuesta 92/C 156/03 DOCE 156/4 de 23 de Junio de 1992.

nales sólo tiene legitimidad cuando está ligado al logro de fines lícitos y legítimamente aceptables para una actividad determinada. Además, la Ley refuerza los controles y garantías estableciendo el régimen de responsabilidad de sus titulares y responsables en cuanto empresarios o trabajadores del mismo. En este campo donde cobra carta naturaleza la aplicación de las normas del derecho del consumo a los usuarios de los ficheros privados, por cuanto la responsabilidad del titular frente al usuario de los ficheros tiene plena naturaleza contractual, mientras que la responsabilidad civil por los daños, morales o materiales, ocasionados a las personas afectadas por el fichero tiene pleno carácter extracontractual y naturaleza objetiva, pudiendo aplicarse en este caso los dictados del moderno derecho de Daños surgido de las normas del Código Civil, así como futuras normas relativas a responsabilidad por productos defectuosos y por la prestación de servicios.

En cuanto al régimen de responsabilidad de la Administración y sus funcionarios, en relación a los ficheros de titularidad pública, debemos atender a lo dispuesto en el Título X, artículos 139 y siguientes de la precitada L.R.J.A.P. y P.C.C. de 26 de Noviembre de 1992 que cubre las lesiones a bienes y derechos de los ciudadanos, salvo casos de fuerza mayor, como consecuencia del funcionamiento normal o anormal de los servicios públicos, completada con las normas ya comentadas de la propia LORTAD sobre la materia.

VII. Conclusiones.

De todo lo que antecede podemos deducir la consagración de un nuevo derecho fundamental a la libre autodeterminación informática, en cuyo seno se conjugan, a modo de haz, un conjunto de posibilidades de actuación vertebradas en verdaderos derechos subjetivos, cohexionados entre sí, que funcionan a modo de garantías que aseguran el pleno disfrute de valores esenciales de la persona, dignidad, honor, fama y privacidad, así como el libre ejercicio de todos sus derechos. Con ello se cumple un mandato constitucional que busca una meta superior a la simple limitación del uso de una nueva tecnología, sino el consagrar una esfera de libertad de la persona frente a los detentadores de este auténtico instrumento de poder en que puede convertirse la informática. Ello se vertebra, fundamentalmente, a través de una Ley Orgánica, como debe ser cuando se trata de derechos fundamentales, pero esta norma, con ser necesaria y aportar novedades interesantes, contiene también defectos de entre los cuales cabe destacar el hecho de que la "Razón de Estado" impone múltiples limitaciones al ejercicio de tan capital derecho, algunas de las cuales se nos antojan de dudosa legalidad.

No obstante, el transcurso del tiempo permitirá a los juristas interpretar la norma en el sentido más acorde a la sensibilidad de la realidad social del momento, de tal manera que conceptos como "privacidad", datos sensibles o interés general irán siendo interpretados de forma ampliadora en beneficio de las garantías y derechos que al ciudadano competen, de manera que se posibilite un cada vez más amplio campo de actuación a la libertad de las personas.

Comentario a la S.T.C. 254/1993, de 20 de Julio. Algunas Reflexiones en torno al Artículo 18.4 de la Constitución y la Protección de los Datos Personales

ANA ROSA GONZALEZ MURUA
Profesora de Derecho Constitucional.
Facultad de Derecho de la Universidad del Pais Vasco.

I. Antecedentes del Caso[1]

Mediante escrito de 28 de febrero de 1986 presentado el siguiente 5 de marzo el Sr. D. Francisco Javier Olaverri Zazpe solicitó al Gobernador Civil de Guipúzcoa se le comunicara si la Administración del Estado o cualquier organismo de ella dependiente disponía de ficheros automatizados donde figuraran sus datos personales. En caso afirmativo solicitaba, asimismo, que se le indicara la finalidad principal de dichos ficheros, la autoridad que los controlaba y su residencia habitual, y que toda esta información relativa a los datos

1 Esta sentencia ha sido publicada en el Boletín Oficial del Estado, nº 197. Suplemento de 18 de Agosto de 1993, pp. 28 y ss.

existentes en dichos ficheros relativos a su persona, se le comunicara de forma inteligible[2] y sin demora.

Denunciada la mora, el actor elevó alzada ante el Ministerio del Interior. Tras ello, interpuso recurso judicial, que fue desestimado tanto en la instancia de la Audiencia Territorial de Pamplona (sentencia de 7 de febrero de 1989) como por el Tribunal Supremo (sentencia de 30 de abril de 1990).

Contra la denegación presunta del Gobernador Civil de Guipúzcoa y del Ministro de Interior así como contra las citadas sentencias que confirmaron la denegación administrativa, el Sr. Olaverri, mediante escrito registrado el 14 de julio de 1990, interpuso recurso de amparo alegando que esta negativa de la Administración vulneraba los artículos 18.1 y 18.4 de la Constitución.

El 20 de julio de 1993, cumplidos tres años desde su interposición, el Tribunal Constitucional otorga el amparo solicitado y en consecuencia: Anula la denegación administrativa de la información así como las sentencias mencionadas y declara el derecho del actor a que las autoridades administrativas demandadas le comuniquen sin demora la información en los términos que el Tribunal expresa en el fundamento jurídico noveno de esta sentencia.

Conocido el fallo y antes de entrar en el análisis de los aspectos más interesantes de esta sentencia, conviene recordar que poco antes de que se conceda este amparo se produce un hecho fundamental en la materia, a saber, el desarrollo legislativo, mediante ley orgánica del artículo 18.4, uno de los pocos preceptos constitucionales que a esas alturas no había sido objeto de regulación por el legislador [3].

II. La Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal.

El 31 de enero del presente año ha entrado en vigor la Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal (LOR-

- 2 En la publicación de la sentencia en el B.O.E. aparece el término "inteligente". Se trata de una errata que hay que sustituir por la palabra "inteligible".
- 3 Y más concretamente "una de las pocas leyes previstas en el Capítulo II, Sección Primera del Título I de la Constitución que no ha sido aprobada hasta ahora", como pone de manifiesto P. LUCAS MURILLO DE LA CUEVA, "la protección de los datos personales ante el uso de la informática en el derecho español" (I parte) en la revista Estudios de Jurisprudencia, ed. Colex, nº 3, Noviembre/ Diciembre 1992, p.8.

TAD)[4] · A pesar de ser España uno de los pocos países en Europa que reconoce constitucionalmente la necesidad de proteger los datos personales ante el uso de la informática[5] -el artículo 18. 4 de la Constitución establece 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 los derechos"- ha sido necesario esperar catorce años para ver cumplido este mandato constitucional [6].

Durante todo este largo período se ha venido asistiendo al fracaso de distintas iniciativas legislativas, alegándose siempre que el Gobierno ya tenía preparado un anteproyecto de ley sobre la materia[7]. Pero la promesa gubernamental se ha ido retrasando hasta que, motivos de otra índole, le han obligado prácticamente a sacar esta Ley adelante. La adhesión de España a los acuerdos de Schengen que le comprometen a intercambiar con las policías de otros países información personal, las normas para la protección de datos personales trasnacionales que prepara el Consejo de Europa, y la Propuesta de Directiva Comunitaria, la cual inmediata y automáticamente a partir de su aprobación formará parte del ordenamiento jurídico interno, han determinado que España necesite aprobar esta normativa si no quiere quedar excluido de este espacio uniforme[8].

- 4 Esta Ley fue sancionada y promulgada el 29 de Octubre de 1992 y publicada en el Boletín Oficial del Estado de 31 de Octubre de 1992, sin embargo la LORTAD no ha entrado en vigor hasta la fecha indicada de 31 de enero de 1993, ya que conforme a su disposición final cuarta: "la presente Ley Orgánica entrará en vigor a los tres meses de su publicación en el "Boletín Oficial del Estado".
- 5 Con anterioridad, la Constitución portuguesa de 1976 dedica, dentro de su Título II relativo a los derechos y libertades, un artículo (art. 35) al uso de la informática. Sin embargo, no hace mucho tiempo que se ha regulado este precepto (Ley 10/91, de 9 de abril sobre la protección de datos personales frente a la informática). Por su parte, en Austria, mediante un procedimiento que posibilita insertar disposiciones constitucionales en leyes ordinarias, el artículo 1 de la Datenschutzgesetz (ley federal sobre protección de datos personales), que declara el derecho fundamental a la protección de los datos personales, ha sido elevado a rango constitucional.
- 6 Conviene aclarar que, como viene siendo práctica frecuente nos hallamos ante un supuesto de ley parcialmente orgánica. Por ello, a pesar de que la Ley sea denominada como orgánica varios de sus preceptos conforme a su disposición final tercera poseen el rango de ley ordinaria.
- 7 En todos estos años, como texto oficial el gobierno sólo había presentado en 1984 el Anteproyecto de Ley Orgánica de regulación del uso de la informática para la protección de los datos personales, pero su tramitación fue suspendida. Distintos estudios se han venido ocupando de este anteproyecto y de cada una de las iniciativas legislativas, la enumeración de todos ellos sería bastante prolija. Por ello, vid. por todos, "Protección de Datos Personales" (Documentación preparada para la tramitación del Proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal). Secretaría General del Congreso de los Diputados. Documentación nº 87, vol. 1, Septiembre, 1991 -donde se encuentran recogidos los precedentes parlamentarios, las proposiciones de ley presentadas durante todas las legislaturas, así como las proposiciones no de ley, las comparecencias y las preguntas escritas y orales en torno a la ausencia del desarrollo legislativo del art. 18- y A. E. PEREZ-LUÑO "Los derechos humanos en la sociedad tecnológica", en el libro de M. LOSANO, A. E. PEREZ-LUÑO y M. F. GUERRERO MATEUS "Libertad informática y leyes de protección de datos personales", Cuadernos y debates, nº 21, Centro de Estudios Constitucionales, Madrid, 1989, pp. 185 y ss., quien reúne y analiza no sólo las distintas iniciativas y proyectos institucionales sino también diversas propuestas doctrinales. 8 A estas circunstancias habría que añadir el escándalo que se originó tras el descubrimiento por la policía de una red que traficaba con datos personales procedentes, según todo indica, de ficheros automatizados de titularidad pública. Sobre este particular resulta sumamente ilustrativo la comparecencia del Ministerio de Justicia ante la Comisión Constitucional del Congreso de los Diputados, véase para ello el Diario de Sesiones del Congreso de los Diputados, Comisiones, IV Legislatura, nº 380, de 11 de febrero de 1992.

El retraso de la Ley podría verse compensado, si nos hallásemos ante una Ley moderna, la cual se estaba beneficiando ("por ello la tardanza", se justificaba el Gobierno) de la evolución de la doctrina jurídica vertida tanto en las normas dictadas a nivel internacional como en el marco de los "Estados" que habían legislado en esa materia. Sin embargo, el panorama que abre la LORTAD es bien distinto. La Ley recibe continuas críticas durante todo su iter legislativo. Numerosas excepciones, como la posibilidad de que datos sensibles sean recogidos y tratados por las Fuerzas y Cuerpos de Seguridad sin ser necesario el consentimiento del afectado, o la dependencia gubernamental del Director de la Agencia de Protección de Datos, por citar algunos de entre los abundantes ejemplos, ponen en cuestión el verdadero objeto de la misma: la protección de los datos personales ante el uso de la informática. Prueba de ello es que nada más entrar en vigor, ha sido objeto de cuatro recursos de inconstitucionalidad, presentados por el Defensor del Pueblo, el Consejo Ejecutivo de la Generalidad de Cataluña, el Parlamento de esta misma Comunidad y el Grupo Parlamentario Popular[9].

Llegado a este punto, y a pesar de la opinión generalizada, y a mi entender fundada, de que esta Ley ha nacido tarde y mal. Lo cierto es que, y enlazando con el análisis del recurso de amparo que será centro de nuestra atención durante las siguientes páginas, la LORTAD ofrece, a primera vista, una vertiente positiva al regular una serie de principios, como por ejemplo:

- Los principios de pertinencia, exactitud, actualización, racionalidad y congruencia de los datos o,

■ 9 En el Boletín Oficial del Estado nº 43, de 19 de febrero de 1993, p. 5259, se recoge la admisión a trámite de estos recursos. Varios autores han analizado y criticado ciertos puntos de la ley, desde que era un proyecto hasta su conversión en texto definitivo. Vid, por todos, D. LOPEZ GARRIDO, "El Proyecto de Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal: la excepcionalidad como norma" en Jueces para la Democracia nº 13, nº2/1991, pp.17 y ss. y J. J. TASENDE CALVO, "Notas al proyecto de ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal", en Poder Judicial, nº 231/1991, pp. 105 y ss. Sobre la LORTAD merece destacar entre otros, M. HEREDERO HIGUERAS, "La ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Introducción general", en Boletín de Información del Ministerio de Justicia, nº 1669, de 25 de abril de 1993, pp. 2090 y ss., así como la obra citada de P. LUCAS MURILLO DE LA CUEVA, "La protección de los datos personales ante el uso de la informática" (I parte) en la revista Estudios de Jurisprudencia, ed. Colex, nº 3, noviembre/diciembre 1992, pp.7 y ss. y (II parte) en esta misma revista nº 4, enero/febrero 1993, pp. 7 y ss. y la más reciente publicación de este mismo autor "Informática y Protección de datos personales (Estudio sobre la ley orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)" en Cuadernos y Debates, nº 43, Centro de Estudios Constitucionales, Madrid, 1993.Por otra parte hay que destacar la importante labor de la CLI (Comisión de Libertades e Informática), cuyo documento relativo a propuestas de enmienda a este proyecto de Ley, influyó enormemente en las diferentes enmiendas presentadas por los grupos parlamentarios. También ha jugado un papel decisivo para que el Defensor del Pueblo presentara recurso de inconstitucionalidad a esta Ley (su labor continúa, denunciado y proponiendo soluciones con el fin de conseguir el efectivo cumplimiento de la LORTAD de la forma más protectora para los derechos y libertades).

- El principio del consentimiento del interesado para el tratamiento automatizado de los datos[10].

Principios que encuentran su manifestación correspondiente, su eficacia jurídica en una serie de derechos entre los que cabe citar entre otros:

- El derecho de información, consistente en la facultad de conocer la existencia de ficheros automatizados de carácter personal, sus finalidades, la identidad del responsable del fichero y su residencia habitual.

- El derecho de acceso que se define como la facultad del titular para solicitar y obtener del responsable de un fichero automatizado información sobre sus datos personales que consten en los registros de éste.

- El derecho de rectificación y cancelación, mediante los cuales se le otorga al titular la facultad de corregir aquellos datos inexactos o incompletos así como la posibilidad de eliminar los innecesarios o los que hayan dejado de ser pertinentes para la finalidad para la cual hubieran sido registrados[11].

La situación en 1986, cuando el demandante solicita la información que le es denegada y las situaciones, que en principio pueden vivir las personas a partir de la entrada en vigor de la Ley, son teóricamente distintas. En cualquier caso, se observará la cautela con la se han hecho las afirmaciones anteriores "en principio", "teóricamente". Los problemas antes apuntados pueden hacer que en la práctica estos principios y derechos de los que gozan las personas sean fácilmente exceptuados. La propia Ley así denomina a su artículo 21: "Excepciones a los derechos de acceso, rectificación y cancelación" y a su artículo 22: "Otras excepciones a los derechos de los afectados", algunos de los preceptos que han sido tachados de inconstitucionales.

Visto someramente el panorama que ofrece la LORTAD pasamos al estudio de los siguientes puntos:

- La pretensión del demandante y la situación en 1986: la ausencia de desarrollo legislativo del art. 18.4. La aplicabilidad del Convenio 108.

- Los derechos de información y acceso. La situación antes y después de la entrada en vigor de la LORTAD.

■ 10 Estos principios se encuentran recogidos en el Título II de la Ley denominado "Principios de la protección de datos".
■ 11 La LORTAD dedica su Título tercero a estos derechos de las personas.

- El derecho a la intimidad, y el derecho a la autodeterminación informativa. Otras denominaciones: el derecho a la libertad informática y el derecho a la privacidad. La posición del Tribunal Constitucional.

III. La Pretensión del Demandante y la Ausencia de Desarrollo Legislativo del Art. 18.4.

En la fecha en que el demandante solicita la información, en 1986, ¿cuáles eran las posibilidades de que la pretensión del demandante obtuviera satisfacción, en ausencia de desarrollo legislativo del art. 18.4 CE?.

Una primera solución podría encontrarse en la aplicabilidad directa de la Constitución.

A) LA APLICABILIDAD DIRECTA DE LOS DERECHOS FUNDAMENTALES Y EL SUPUESTO DEL ARTICULO 18.4 DE LA CONSTITUCION.

Sobre este punto, el Tribunal Constitucional en el fundamento jurídico sexto de este recurso de amparo reitera su jurisprudencia consolidada de la aplicabilidad inmediata de la Constitución y así recuerda que "los derechos y libertades fundamentales vinculan a todos los poderes públicos, y son origen inmediato de derechos y obligaciones, y no meros principios programáticos"[12]. Ahora bien, este principio general de aplicabilidad directa puede sufrir excepciones, pero sólamente en dos supuestos: cuando así lo imponga la propia Constitución expresamente o cuando así se deduzca de la naturaleza misma de la norma[13].

De este modo, el Constitucional recuerda que "cuando se opera con una "reserva de configuración legal" es posible que el mandato constitucional no tenga más que un mínimo contenido, que ha de verse desarrollado y completado por el legislador".

Este sería el caso del artículo 18.4, en el cual se produce una remisión a la ley para que limite el uso de la informática en aras a la protección de los derechos. Sin embargo, lo que se trata de ver es si, mientras esta regulación se produzca, el contenido mínimo provisional en relación con este derecho o libertad incluye los derechos a obtener información ejercitados por el demandante.

- 12 Así se pronunció el Tribunal Constitucional en STC 21/81, de 2 de julio, y después reiterada en STC 15/1982, de 23 de abril.
- 13 STC 15/1982, de 23 de abril

Con respecto a ese contenido mínimo provisional resultan interesantes los argumentos del Abogado del Estado, del Fiscal y del Tribunal Constitucional.

Los tres destacan que conforme a su tenor literal, el art. 18.4 posee un contenido negativo: el uso de la informática como límite al honor, a la intimidad de las personas y al pleno ejercicio de los derechos. El Abogado del Estado sostiene que conforme a esta vertiente defensiva se pueda justificar en ciertos casos la negativa de un ciudadano a suministrar a las autoridades determinados datos personales como el origen racial o la vida sexual.

Pero posteriormente las divergencias surgen. Para el Abogado del Estado el art. 18.4 requiere una intervención legislativa, y mientras no se dé, falta la organización necesaria para asegurar la protección. Por tanto, no es posible en ausencia de desarrollo legislativo satisfacer la petición del demandante. La garantía del 18.4 opera sólamente en su vertiente negativa y no como título para solicitar deberes prestacionales a los poderes públicos.

Sin embargo, el Tribunal Constitucional añade, siguiendo lo expuesto por el Ministerio Fiscal, que la garantía de la intimidad adopta hoy, además de un derecho a negar información sobre los datos personales, "un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)".

Esta es la concepción positiva pero ¿cuál es la vía argumental utilizada por el TC para concluir que la pretensión del Sr. Olaverri, que los derechos de información y acceso por él solicitados forman parte del contenido mínimo del 18.4 CE, y que en ausencia de este desarrollo legislativo gozan de eficacia directa?. Y es aquí donde entra en juego la segunda solución, (que en el fondo se convierte en premisa de la primera): el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

El Tribunal realiza el paso de una concepción negativa de este derecho a una positiva gracias a la interpretación del citado Convenio:

"...la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria positiva, y es aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España" (fundamento jurídico séptimo).

B) LA APLICACION DEL CONVENIO 108.

El Sr. Olaverri fundó su solicitud en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, el cual había sido publicado en el Boletín Oficial del Estado de 15 de noviembre de 1985, y por tanto conforme al art. 96.1 de la Constitución quedaba incorporado al ordenamiento jurídico interno[14].

La petición del demandante reproduce prácticamente los dos primeros apartados del art. 8 del Convenio a cuyo tenor cualquier persona deberá poder:

"a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero.

b) Obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernen a dicha persona, así como la comunicación de dichos datos de forma inteligible"[15].

Ahora bien, como afirma el Tribunal "el nudo gordiano del presente recurso consiste en determinar si las dos primeras letras del art. 8 del Convenio del Consejo de Europa sobre protección de datos personales surten efecto directo, o en su caso interpretativo, en relación con los derechos fundamentales que enuncia el art. 18 de la Constitución" (fundamento jurídico cuarto).

Comencemos por la primera vía, la eficacia inmediata del Convenio.

■ 14 El art. 96.1 de la Constitución establece que: "Los tratados internacionales válidamente celebrados, una vez publicados oficialmente en España formarán parte del ordenamiento interno". Como hemos visto el requisito de la publicación se produjo el 15 de noviembre de 1985, (Boletín Oficial del Estado nº 274), sin embargo, para el 1 de octubre de 1985 se trataba de un texto válido y vigente. Esto obedece a las siguientes circunstancias: El plenipotenciario del Estado español había firmado este Convenio en Estrasburgo el 28 de enero de 1992, y fue el cuarto país en ratificarlo el 27 de enero de 1984. Su entrada en vigor quedaba condicionada conforme a su artículo 22:
-En primer lugar, a que fuera ratificado, aceptado o aprobado por cinco Estados miembros del Consejo de Europa. El quinto Estado en ratificarlo fue la República Federal de Alemania el 19 de junio de 1985.
-En segundo lugar, para la entrada en vigor, la fecha concreta sería el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha en que este quinto Estado quedaba vinculado. Como se puede comprobar se trata del 1 de octubre de 1985.

■ 15 En 1987, posiblemente en relación con este "asunto", el Sr. Bandrés Mollet como portavoz del Grupo Parlamentario Mixto presentó una proposición no de ley relativa al cumplimiento por el Gobierno de las obligaciones derivadas del Convenio 108 del Consejo de Europa, sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. En ella denunciaba que el Gobierno español negaba a los ciudadanos el derecho a acogerse a las disposiciones del Convenio, contestando negativamente a los requerimientos que éstos hacían en relación al ejercicio del derecho de acceso a los ficheros automatizados al amparo del artículo 8 de este Tratado. Para la consulta de esta proposición vid. Boletín Oficial de las Cortes Generales. Congreso de los Diputados, Serie D: Actos de control, III Legislatura, nº 49 de 18 de marzo de 1987.

Como se señaló en los antecedentes, tanto la Audiencia Territorial de Pamplona como el Tribunal Supremo confirmaron la presunta denegación administrativa del Gobernador Civil de Guipúzcoa y del Ministro de Interior, de la comunicación de la información solicitada. Sus argumentaciones se basaban fundamentalmente en la inaplicabilidad directa del Convenio.

Así para la Audiencia los preceptos del Convenio no son aplicables directamente. La aplicación se halla supeditada a la adopción por cada parte, en su derecho interno, de las medidas necesarias para que los principios básicos para la protección de datos alcancen efectividad, de acuerdo con lo que establece el art. 4.1 del propio Convenio. Previsión coincidente con la del art. 94.1.e) de la Constitución, acerca de que la ejecución de los tratados o convenios puede exigir medidas legislativas[16].

Por su parte, el Tribunal Supremo confirmó que el Convenio necesita para su aplicación práctica el complemento de una actividad interna legislativa y reglamentaria que el Estado no ha desarrollado todavía[17].

Siguiendo esta línea de la Audiencia Territorial de Pamplona y del Tribunal Supremo, desde la doctrina se ha mantenido que este Convenio no es directamente aplicable y se ha precisado que su virtualidad consiste en obligar al Estado Español ante los demás firmantes del mismo a que proceda a su desarrollo[18].

- 16 Por su parte en la memoria explicativa que acompaña al texto del Convenio publicado por la Presidencia del Gobierno, se dice que este Tratado no ha sido concebido como self executing y que por consiguiente los derechos de los individuos no pueden derivarse directamente de él. Lo cierto es que las medidas necesarias para dar cumplimiento al Convenio deberían haber estado en vigor en el momento en que dicho Tratado surtiera efecto en el Estado español, y por tanto, se ha producido un vacío jurídico que no debería haber ocurrido. Véase la nota 13 de la publicación "Protección de Datos. Convenio del Consejo de Europa de 1981" en Documentación Informática, serie amarilla/Tratados internacionales nº 3. Presidencia del Gobierno. Servicio Central de Publicaciones. Servicio Central de informática, Madrid, 1983, p. 31.
- 17 Con respecto al papel que han de desempeñar los jueces en la aplicación del Convenio 108, mientras no existan instituciones de control que garanticen los derechos de las personas como los que aquí analizamos, (derecho de información, derecho de acceso, etc) A. E. PEREZ-LUÑO, en su artículo: "Los derechos humanos en la sociedad tecnológica. . .", cit., concretamente en la página 180 dice: " Preciso es decir que abogar por la creación de instituciones de garantía de los derechos y libertades establecidos en el Convenio europeo no supone ignorar o infravalorar la importante labor que en ello compete a los tribunales de justicia. El texto del Convenio, por ser parte de nuestro ordenamiento jurídico, es norma directamente invocable ante y aplicable por la judicatura española. Es más, en el momento actual, y ante la carencia de instituciones básicas con que cuentan los ciudadanos de nuestro país para ver paulatinamente protegidos sus derechos y libertades frente a eventuales abusos perpetrados desde los bancos de datos o ficheros automatizados. Ello se logrará a través de una decidida y adecuada aplicación de la normativa del Convenio europeo por nuestros jueces".
- 18 Vid P. LUCAS MURILLO DE LA CUEVA, "La protección de los datos personales ante el uso de la informática en el derecho español" (I parte)...cit., p.10. Este autor toma como base precisamente para mantener esta postura la sentencia del Tribunal Supremo relativa al "caso" que estamos estudiando de 30 de abril de 1990. Partiendo de esta misma sentencia llega a igual conclusión M. A. DAVARA RODRIGUEZ, "Derecho Informático", Ed. Aranzadi, Pamplona, 1993, p.64. Por otra parte, sobre la incorporación de este Convenio al ordenamiento jurídico español se han dedicado varios estudios pero centrándonos en el problema relativo a su aplicabilidad directa merece destacarse, además de a los autores recién mencionados, a G. GARZON CLARIANA, "La protección de los datos personales y la función normativa del Consejo de Europa" en Revista de

En este sentido el TC considera cuestión ajena al recurso de amparo la alegación que el demandante fundaba en el art. 96.1 CE, según la cual razonaba el efecto directo del artículo 8. del Convenio.

"La adecuación de una norma legal, o de una disposición o actuación de los poderes públicos, a lo preceptuado por un tratado internacional, y por consiguiente si las autoridades españolas han cumplido o no los compromisos derivados de un acuerdo internacional, son cuestiones que, en sí mismas consideradas, resultan indiferentes para asegurar la protección de los derechos fundamentales comprendidos en el art. 53.2 C.E., que es el fin al que sirve la jurisdicción de este Tribunal en el ámbito del recurso de amparo" (fundamento jurídico quinto) .

Sin embargo, el TC se decanta por el valor interpretativo del Convenio:

"...los textos internacionales ratificados por España pueden desplegar ciertos efectos en relación con los derechos fundamentales, en cuanto pueden servir para configurar el sentido y alcance de los derechos recogidos en la Constitución, como hemos mantenido, en virtud del art. 10.2 C.E., desde nuestra STC 38/81, fundamentos jurídicos 3° y 4°. Es desde esta segunda perspectiva desde la que hay que examinar la presente demanda de amparo" (fundamento jurídico sexto).

Como se ha señalado en el epígrafe anterior, las pautas interpretativas del Convenio 108 permiten considerar que la pretensión del demandante se encuadra perfectamente dentro del contenido mínimo, -en ausencia de desarrollo legislativo- del artículo 18 de la Constitución.

En opinión del Tribunal tanto los problemas a los que se tuvo que enfrentar la elaboración y la ratificación de este Tratado, como la experiencia de los países del Consejo de Europa que se condensa en su articulado, conducen a la conclusión de que la protección de la intimidad debe incluir la facultad de que los ciudadanos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados de las Administraciones Públicas donde se conservan datos de carácter personal que les conciernen, así como cuáles son esos datos personales que obran en poder de las autoridades .

Instituciones Europeas, vol.8, nº 1, enero-abril 1981, p.18, quién opina que no se puede afirmar con rotundidad el carácter no self executing del Convenio 108, a M. HEREDERO HIGUERAS, "Ante la ratificación del Convenio de protección de datos del Consejo de Europa" en Documentación Administrativa, nº 199, julio-septiembre y octubre-diciembre 1983, p.754, y más recientemente en "La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado..." cit., p. 2090, así como a A. E. PEREZ-LUÑO, "Los derechos humanos en la sociedad tecnológica... ", cit., especialmente p.175 y p.180.

Sin embargo, esta argumentación utilizada por el TC es criticada por el Presidente del Tribunal don Miguel Rodríguez-Piñero y Bravo-Ferrer en su voto particular formulado en este recurso de amparo. Dicho magistrado discrepa del criterio mayoritario, ya que en su opinión, en este caso el Convenio no se ha utilizado meramente, frente a lo que se dice " como una fuente interpretativa que contribuye a la mejor interpretación del contenido de los derechos..., sino como elemento de integración ante la demora en el desarrollo legislativo del precepto constitucional, para cuyo desarrollo desde luego habría de servir de pauta, aunque no canon autónomo de validez, el contenido de dicho Convenio".

Por otra parte, las premisas de las que parten el Abogado del Estado, el Tribunal Constitucional y su Presidente en el voto particular les hace llegar a conclusiones diferentes.

Como hemos visto, en opinión del Abogado del Estado el art. 18.4 CE, a falta de desarrollo legislativo, sólo contiene un mínimo esencial de carácter defensivo, (la negativa del ciudadano en determinados casos, a suministrar ciertos datos) pero nunca supone un derecho activo de control, un derecho prestacional el cual necesita insoslayablemente medidas de Derecho interno.

La petición del recurrente supone una "conducta positiva del Gobierno Civil y del Ministerio de Interior, una prestación informativa (facere)" sólo se hubiera podido satisfacer si se hubiera producido una intervención legislativa previa, que hubiera organizado las garantías complementarias previstas en el art. 8 del Convenio. En conclusión, el derecho fundamental a la intimidad no tiene porque incluir derechos de prestación.

Para el Tribunal Constitucional, sin embargo, el derecho de la intimidad no se agota en unas facultades negativas sino que, merced a las pautas interpretativas del Convenio 108 y como recoge su artículo 8, ha de contener facultades positivas y activas de información y de control sobre la existencia, fines y responsables de los ficheros públicos automatizados de la Administración Pública, tal y como solicitaba el demandante. Estas facultades de información forman parte del derecho a la intimidad, que vincula directamente a todos los poderes públicos, y ha de ser salvaguardado aunque no se haya desarrollado legislativamente.

Por tanto, para el Tribunal no es convincente el Abogado del Estado cuando dice que opera este derecho con contenido negativo, no como derecho de prestación. "No se ve la razón por la que no podría justificar igualmente que ese mismo ciudadano se oponga a que esos mismos datos sean conserva-

dos una vez satisfecho o desaparecido el legítimo fin que justificó su obtención por parte de la Administración, o a que sean utilizados o difundidos para fines distintos, y aun ilegales o fraudulentos, o incluso a que esos datos personales que tiene derecho a negar a la Administración sean suministrados por terceros no autorizados para ello" (fundamento jurídico séptimo).

Expuestos estos argumentos, el Tribunal estima el recurso y considera vulnerado el derecho del art. 18 por la Administración al negar la petición de información solicitada para el demandante[19].

Por su parte, el voto particular, como hemos visto, se aparta del criterio de la mayoría, y en parecida línea a la sostenida por el Abogado del Estado mantiene que, el artículo 18.4, en ausencia del desarrollo legislativo de este mandato constitucional y no pudiendo el Convenio hacer las veces de dicha legislación necesaria, sólo permitiría amparar supuestos como pueden ser la negativa de la persona a suministrar determinados datos a la Administración (lo que hemos denominado vertiente defensiva) pero nunca crear una obligación de hacer para la Administración, una conducta positiva sin previa base legal (negando de esta manera la vertiente positiva, la posibilidad de ejercitar los derechos de información, acceso...).

Esto conduce a la conclusión de que ni la Administración ni el órgano judicial han vulnerado el derecho fundamental del recurrente al negar la aplicación directa del Convenio. Sólo a partir de la entrada en vigor de la LORTAD, los derechos reconocidos en dicha Ley, - en el supuesto que nos ocupa

■ 19 El diputado socialista DIAZ FORNAS en la toma en consideración de la Proposición de Ley del Grupo parlamentario de Coalición Popular sobre protección al honor y a la intimidad frente a la utilización de las bases de datos decía que, a pesar de la exigencia de una ley de protección de datos, tanto por el art. 18.4 CE como por la obligación contraída por el Convenio 108, en su ausencia no se tenía que producir una situación de indefensión ya que el derecho a la intimidad, el honor y los derechos que atañen a la privacidad, tiene el rango de fundamentales y cuentan con la protección reforzada del artículo 53.2 de la Constitución, el recurso de amparo ante el Tribunal Constitucional. Si se interpreta que el derecho a la privacidad ,- como posteriormente veremos-, posee también la vertiente activado de control del derecho, manifestada en el derecho de información, de acceso, de rectificación, etc, se podría llegar a la conclusión de que también éstos últimos podrían gozar de la protección de amparo constitucional. Vid, esta solución en el Diario de Sesiones del Congreso de los Diputados, Pleno y Diputación Permanente, III Legislatura, n°99, de 12 de abril de 1988, p. 6145. Posteriormente, y en respuesta de la proposición no de ley presentado por el Sr. Bandrés citada en nota 15, este mismo diputado sostiene que "..si bien el conjunto de principios establecidos en el convenio deben ser desarrollados por la legislación interna para su plena efectividad, algunos de sus preceptos como bien pudieran ser los que contiene su artículo 8°, podrían aplicarse directamente para contener derechos de las personas, y de acuerdo con nuestro sistema constitucional."
Sorprende esta interpretación teórica que no deja de ser positiva (si bien utilizada, en mi opinión, para eludir las obligaciones contraídas por el Convenio y justificar la tardanza en la regulación legislativa del art. 18.4 CE). Sin embargo, a renglón seguido añade que ni el Estado español ni el Gobierno niegan ni vulneran los derechos de los ciudadanos". Como hemos tenido ocasión de comprobar esta interpretación teórica no ha sido llevada a la práctica, por lo menos en el caso" que nos ocupa. Para su consulta véase el Diario de Sesiones del Congreso de los Diputados, Comisiones, III Legislatura, n°92, de 11 de marzo de 1987, p.3601.

serían los derechos de información y de acceso - en cuanto desarrollo del derecho a la intimidad, pueden ser objeto de tutela y protección a través del recurso de amparo, pero no antes.

Pero, sin embargo el Tribunal Constitucional como consecuencia de los argumentos arriba apuntados declara el derecho del actor a que el Gobernador Civil le comunique sin demora la información solicitada, que incluye los siguientes extremos:

-La existencia de ficheros automatizados de datos de carácter personal, dependientes de la Administración Civil del Estado, así como sus finalidades, y la identidad y el domicilio de la autoridad responsable del fichero.

-La comunicación en forma inteligible de aquellos datos personales que al actor le conciernen, pero tan sólo los contenidos en ficheros sobre los que el Gobernador civil sea competente.

Una última observación. El Tribunal Constitucional antes de declarar el derecho del demandante a la petición informativa solicitada debe superar una objeción más del Abogado del Estado: la imposibilidad material, la carencia de los medios precisos, en que se encuentran las autoridades para poder satisfacer la pretensión del demandante.

A lo que el Tribunal responde:

"El que un determinado órgano administrativo disponga, o carezca, de los medios materiales o de las atribuciones competenciales precisos no sirve para discernir los derechos de un ciudadano, especialmente si esos derechos son declarados por la Constitución" (fundamento jurídico tercero).

Por lo tanto, como el actor tiene derecho en virtud del art. 18 a ver satisfecha su petición, será deber de todos los poderes públicos poner los medios organizativos y materiales para procurársela. De todos modos, esta cuestión deberá matizarse cuando tratemos el ejercicio del derecho de información y el del derecho de acceso.

Además, añade el Tribunal que el Gobernador Civil como representante permanente del Gobierno de la Nación en la provincia, así como primera autoridad de la Administración Civil del Estado detenta la competencia para "ejercer la superior dirección de todos los servicios periféricos de dicha Administración en la provincia, y coordinar la actividad de todos sus órganos". Por consiguiente, el Gobernador Civil era plenamente competente para resolver la

petición solicitada por el actor y en cualquier caso, nunca esas carencias administrativas pueden servir de justificación para mantener su silencio.

IV. Los Derechos de Información y Acceso. La situación antes y después de la entrada en vigor de la LORTAD.

Recordemos la pretensión del demandante, el actor solicitaba el derecho a conocer si existen ficheros automatizados de la Administración del Estado o de cualquier organismo de ella dependiente, donde figuraran sus datos personales, y en caso afirmativo, se le indicara la finalidad principal de estos ficheros, la autoridad responsable y su residencia habitual, y que toda esta información relativa a los datos existentes en dichos ficheros relativos a su persona, se le comunicara de forma inteligible y sin demora.

El TC se aparta en parte de la pretensión del demandante, distinguiendo lo que las legislaciones de protección de datos, (asimismo la reciente LORTAD) y el propio Tribunal en esta sentencia denomina, el derecho de información y el derecho de acceso. Cuando enumeramos los derechos que establece la L.O. 5/1992, de 29 de octubre, dijimos que el derecho de información, se viene concibiendo como un derecho general a poder conocer qué ficheros automatizados existen, su finalidad, la identidad del responsable y su residencia habitual, mientras que el derecho de acceso consiste en la facultad del titular para solicitar y obtener información sobre sus datos personales que consten en los ficheros automatizados.

Por su parte, de la pretensión del actor se deduce lo siguiente: El Sr. Olaverri pedía al Gobernador Civil que le comunicara la totalidad de sus datos personales que se contenían en todos y cada uno de los ficheros de la Administración del Estado. La pretensión así formulada difícilmente podía prosperar.

Veámos el precepto que el Convenio 108 dedica al derecho de información y de acceso, y en el cual se inspiró el demandante:

" Cualquier persona deberá poder:

a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero.

b) Obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter

personal que conciernen a dicha persona, así como la comunicación de dichos datos de forma inteligible.

El apartado a) se refiere al derecho de información mientras que el b) queda dedicado al derecho de acceso[20] . Lo cierto es que de la letra del Convenio no resulta fácil deducir -y por tanto tampoco para el demandante- cómo se debe proceder para poder ejercitar estos derechos. Por otra parte, como ya se puso de manifiesto, tampoco se puede exigir más a un Convenio que lo que pretende es establecer en este punto unos mínimos que debían haber sido desarrollados en la legislación interna antes de su entrada en vigor. Sin embargo, y aun en ausencia de desarrollo legislativo en esas fechas en España, el derecho comparado y la doctrina que para aquél entonces ya se habían acercado al estudio de estos temas proporcionaban un auxilio considerable en la interpretación de este artículo.

Así, en las Jornadas internacionales sobre Informática y Administración Pública, organizadas por el IVAP/HAEE, HERNANDO COLLAZOS en su estudio titulado "La Comunidad Económica Europea y la Informática"[21] dedicaba un capítulo a los aspectos técnicos del derecho a acceder a los datos personales. La autora desglosaba el derecho acceder a los datos en cuatro más específicos:

-El derecho público a conocer la existencia de todos los ficheros.

-El derecho del individuo a conocer la existencia de información que le concierne en un fichero determinado.

-El derecho del individuo a conocer el contenido de la información que le concierne en un fichero determinado.

-El derecho del individuo a solicitar la rectificación de los datos que le conciernen, si es necesario.

Con respecto al primero, el derecho público a conocer la existencia de todos los ficheros, que coincide con lo que hemos denominado derecho a la

■ 20 Por su parte, M. HEREDERO HIGUEŔAS prefiere la expresión "derecho de acceso en sentido amplio" para referirse a lo que se viene denominando derecho a la información y la de "derecho de acceso en sentido estricto" en lugar de la generalmente empleada derecho de acceso. Estas denominaciones las ha venido manejando dicho autor desde hace ya algún tiempo, así con respecto al Anteproyecto de Ley Orgánica de 1984 en su artículo "El anteproyecto de Ley Orgánica de regulación del uso de la informática, cinco años después en Congreso sobre Derecho Informático, Facultad de Derecho, Zaragoza, 1989, p. 284 y en relación a la LORTAD en "La ley orgánica 5/1992, de 29 de octubre...", cit., p. 2099.

■ 21 I. HERNANDO COLLAZOS, " La Comunidad Económica Europea y la Informática" en Jornadas Internacionales sobre Informática y Administración Pública", I. V. A. P./ H. A. E. E., Oñati, 1986, p.87.

información, lo considera una consecuencia del principio de transparencia. Se trata, en definitiva, de un derecho de información general a conocer qué ficheros automatizados existen, de quién dependen, qué fines persiguen, etc. Asimismo distingue las distintas formas que en las legislaciones de protección de datos se contemplan para ejercer este derecho: sistema de información voluntaria por parte de los responsables, de publicación en boletines oficiales o de registro público.

Como se puede comprobar el apartado a) del art. 8 del Convenio no hace alusión alguna a ninguno de estos sistemas mencionados -tampoco es ésta tarea del Convenio sino de los Estados que adopten las medidas necesarias para garantizar el ejercicio de este derecho-. Con todo, lo que resulta evidente, y así lo han venido regulando las distintas legislaciones de protección de datos, el derecho a la información debe quedar limitado a la facultad que a toda persona corresponde de conocer la existencia de todos los ficheros no comprendiendo, por tanto, -como pretendía el demandante-, la facultad de conocer si en todos esos ficheros se contienen datos que a ella le afectan o no. Lo que ocurre, es que, como más tarde veremos, normalmente para los tratamientos automatizados posteriores a la entrada en vigor de la legislación sobre protección de datos se suele establecer un derecho previo a la información de tal manera que las personas sepan a qué ficheros van a ir a parar sus datos[22] . Sin embargo, como ocurre con la pretensión, objeto de estudio, para los tratamientos anteriores a la Ley -y aunque fuera deseable para que no se diera una desigualdad entre los primeros citados y éstos segundos- no se regula esa posibilidad de conocer los datos que a cada uno conciernen sino ejercitando el derecho de acceso ante todos los posibles ficheros automatizados a instancia del interesado[23] .

Continuando con los derechos segundo y tercero, el derecho del individuo a conocer la existencia de información y el derecho del mismo a conocer el contenido de esa información que le concierne en un fichero determinado, la profesora HERNANDO dice que éste adopta formas diversas según las legislaciones, como pueden ser el método de demanda directa ante el responsable de fichero o el de notificación. En cualquier caso, quien "responde" en última ins-

- 22 Así el artículo 27 de la Ley Francesa n°78-17, de 6 de enero de 1978, sobre Informática, ficheros y libertades establece el derecho de las personas a conocer quiénes van a ser los destinatarios, personas físicas o jurídicas, de la información que se les ha solicitado. Se ha manejado la versión de traducción de M. DARANAS PELAEZ, en Boletín de Legislación Extranjera, n° 88-89, enero-febrero 1989, p.3 y ss. Muy en parecida línea se sitúa el artículo 5 de la LORTAD, si bien las excepciones que prevé ponen en peligro esta facultad.
- 23 Una crítica a la falta de información a los afectados y a la imposibilidad de conocer el titular en qué ficheros se encuentra sin tener que ejercitar el derecho de acceso con respecto a los tratamientos anteriores a la Ley se encuentra en M. LOPEZ-MUÑIZ GOÑI, "Los derechos de la personas en la ley de protección de datos personales" en Jornadas Abogacía e Informática. Illustre Col.legi d'Advocats de Barcelona, 1993, p. 92.

tancia del correcto ejercicio de este derecho, como su propio nombre indica es el "responsable" del fichero[24].

El apartado b) del Convenio piensa en estos dos derechos que constituyen propiamente lo que se denomina derecho de acceso, y aunque tampoco especifica -dejando así abierta las distintas posibilidades que en las legislaciones se establezcan- de quien pueda la persona obtener esta información, se deduce claramente del derecho comparado (exceptuando ciertos supuestos en los que se encomienda dicha función a un intermediario o a la autoridad de tutela[25]) que se ha de tratar del responsable de fichero.

Llegado a este punto hay que afirmar, en consecuencia, que tanto el derecho comparado como la doctrina que lo ha estudiado, brindaban argumentos suficientes para distinguir perfectamente entre derecho de información (o derecho a conocer la existencia de los ficheros) y derecho de acceso (o derecho individual a conocer). Por ellos los términos en se redactó la demanda pueden obedecer a los siguientes motivos:

- El desconocimiento de esta distinción. El actor fundamentó su solicitud en los apartados a) y b) del art. 8 del Convenio. La lectura de este precepto puede conducir a conclusiones erróneas. Cuando el apartado a) habla del derecho a "conocer la existencia de un fichero automatizado", aunque se esté utilizando el número singular se refiere a la posibilidad de conocer la existencia de todos los ficheros automatizados. Por otra parte, el apartado b) se refiere a la facultad de conocer la existencia o no en el fichero automatizado de datos de carácter personal que conciernen a la persona, así como la comunicación de dichos datos de forma inteligible. Poniendo en contacto los dos incisos y si lo mismo que en el primer inciso en el segundo se sobreentendiese que cuando se habla de "fichero automatizado" se quiere decir "ficheros automatizados", se podría concluir que se establece una facultad general de conocer la existencia de todos los datos personales de uno que obre en todos los ficheros automatizados. Sin embargo, como hemos expuesto, esta interpretación no viene siendo admitida.

■ 24 La LORTAD define el responsable de fichero como la"persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre su finalidad, contenido y uso del tratamiento" (art. 3.d). En este mismo sentido el artículo 2.d) del Convenio europeo: "persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán".

■ 25 La Ley Francesa n°78-17, de 6 de enero de 1978, sobre Informática, ficheros y libertades establece el acceso indirecto por medio de un intermediario, un médico con relación a los datos médicos (art.40) y la Comisión Nacional de Informática y Libertades (C.N.I.L.) -órgano de tutela de esta Ley- para los tratamientos que afecten a la seguridad del Estado, la defensa y la seguridad pública. Asimismo, en España aunque no ha llegado a ser derecho vigente, hay que destacar el artículo 30 de la Proposición de Ley Orgánica de Izquierda Unida el cual preveía el acceso a través de la Comisión Nacional para la Telemática con respecto a los bancos de datos de los Ministerios de Hacienda, Defensa e Interior.

- Aun no desconociendo la distinción entre el derecho de información y el derecho de acceso, y a pesar de las pautas que se podían encontrar en la doctrina y en el derecho comparado para interpretar estos derechos, la situación en España en 1986 ofrecía serias dificultades para el ejercicio de los mismos. En primer lugar, si bien es cierto que no es una condición previa el derecho de información, (es decir el poder consultar un listado con el nombre de todos los ficheros existentes y de quién responde de cada uno de ellos), para poder ejercitar el derecho de acceso, (si la persona conoce de antemano la existencia de ese fichero se podrá dirigir directamente ante su responsable para que se le comuniquen sus datos) si uno no conoce qué ficheros existen se dificulta enormemente el derecho individual a conocer si en tal o cual ficheros hay registrados datos personales suyos.

En las fechas en que el actor realizó la demanda no se sabía qué ficheros existían, ya que no estaba establecido ningún medio para asegurar el derecho público al conocimiento de todos los ficheros, el derecho a la información. Por otra parte, las personas podían intuir que ciertos datos estarían en mano de ciertas autoridades, pero desde luego se desconocía a quién se hubiesen podido comunicar o ceder.

Ante la falta de este primer mecanismo de conocimiento, (ningún listado, ni ningún registro donde aparecieran los ficheros que existen, y quiénes eran los responsables de los mismos) el actor se decidió a dirigirse al Gobernador Civil, pues él es, en la provincia, la primera autoridad de la Administración Civil del Estado.

Lo que no sabemos es si esta petición obedece a un desconocimiento de lo que es el derecho de información y el derecho de acceso o que, a sabiendas de ella, se aprovecha la coyuntura española para que el Gobernador sea el encargado de comprobar si en todos y cada uno de los ficheros automatizados de la Administración hay datos del Sr. Olaverri y se los comunique, y además sepa posteriormente a quién dirigirse y a dónde para ejercitar en su caso los derechos de rectificación y cancelación. Con ello de una sola gestión se hubiera conocido todas las informaciones que sobre él constan en todos los ficheros de la Administración.

Sin embargo, como ha opinado, el TC, para garantizar el derecho de información hubiese bastado con que el Gobernador Civil le hubiera comunicado al Sr. Olaverri la existencia, el responsable, y la residencia habitual de todos y cada uno de los ficheros automatizados de datos de carácter personal que dependiesen de la Administración Civil del Estado. Eso si, a él correspondería posteriormente la molestia de comprobar ante estos responsables de

fichero -ejercitando así el derecho de acceso- si en los mismos obraban o no datos suyos personales.

En cualquier caso, hay que poner de manifiesto que si bien el Gobernador Civil en 1986 pudiera haber logrado esa información, lo cierto es que si hubiese querido ofrecer al afectado una respuesta adecuada habría encontrado ciertas dificultades. Así, conforme a la disposición final segunda de la LORTAD los ficheros automatizados de las Administraciones Públicas anteriores a la entrada en vigor de la Ley deberán adoptar una disposición de regulación del fichero o adaptar la que existiera. Esto significa que los extremos arriba mencionados (responsable del fichero, domicilio habitual, fines del fichero) -además de otras informaciones conforme al art.18 del texto legal- deberán ser recogidas en una disposición general, quizás porque muchos de estos ficheros no precisan (ni precisaban hace siete años) con claridad todas estas informaciones necesarias.

- En cuanto al derecho de acceso, el Gobernador Civil no podía comunicar la totalidad de los datos personales del Sr. Olaverri que se contenían en todos y cada uno de los ficheros de la Administración. El Gobernador Civil no tenía ni tiene competencia sobre todos los ficheros de la Administración, como dice el Tribunal Constitucional- sólamente le hubiese podido y podrá comunicar al solicitante "en forma inteligible aquellos datos personales que le conciernen, pero tan sólo los que obren en aquellos ficheros sobre los que el Gobernador Civil ostente las necesarias facultades".

Una vez clarificado como debería haber sido resuelta esta petición en 1986 cuando el demandante la solicitó, a tenor de lo que ya para entonces habían sido definidos como derecho de información y derecho de acceso, una precisión debe ser realizada.

Ni mucho menos lo que se pretendía en estos párrafos anteriores era criticar la redacción de la instancia del solicitante, excusada además por los dos motivos arriba apuntados -quizás el desconocimiento del solicitante ya que el texto en que fundamentó su demanda, no aclara realmente el contenido de estos derechos; o quizás porque el solicitante hizo una "petitio" amplia a sabiendas, esperando ver cuál era la reacción de la Administración a falta de los medios que normalmente se establecen para el ejercicio de estos derechos-, sea lo que fuere, muy por el contrario, nuestros elogios a la misma pues, además de sentar un precedente, demuestra la sensibilidad sobre este tema en unas fechas tempranas (no es lo mismo solicitar esta petición en 1986 que en 1993 tras la entrada en vigor de la LORTAD). El actor atreviéndose a ejercitar la vertiente activa de control de los datos personales persigue conseguir, por

otra parte, reavivar la conciencia ciudadana sobre los peligros que la informática conlleva en el disfrute de los derechos y libertades .

Hecha esta precisión y vista cuál debería haber sido la respuesta hace siete años, hay que ser conscientes de que esta sentencia se produce en un momento en que la esperada -y después criticada- LORTAD ha entrado en vigor. Este hecho puede añadir algún elemento nuevo para su comprensión a pesar de que su institución fundamental, la Agencia de Protección de Datos, -encargada de velar por el cumplimiento de la Ley y especialmente los derechos de información, acceso, rectificación y cancelación de los datos personales[26]- no ha comenzado a funcionar. En cualquier caso es preciso analizar el momento actual para conocer cuál es el momento en que este amparo se hace efectivo y las consecuencias para ahora y a futuro que se desprenden de la doctrina de la jurisprudencia constitucional.

Comencemos por el derecho de información. Este derecho público a conocer la existencia de los ficheros, -por medio del cual todas las personas y no sólo los afectados (se trata de un derecho público) pueden conocer qué datos se procesan en una sociedad, quién los realiza, con qué fin-, se ha de configurar como un derecho necesario que ayude a prevenir en lo posible la lesión de los derechos o libertades a partir de un tratamiento automatizado y garantice el principio de transparencia en una sociedad democrática.

Con anterioridad vimos que existen diversos sistemas en las legislaciones de protección de datos para hacer posible el ejercicio de este derecho: sistema de información voluntaria por parte de los responsables, de publicación en boletines oficiales o de registro público. La LORTAD, por su parte, dedica generosamente varios artículos a los diversos medios que se establecen para garantizar el derecho de información.

Artículo 13. Derecho de información.

"Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de ficheros automatizados de datos de carácter personal, sus finalidades y la identidad del responsable del fichero. El Registro General será de consulta pública y gratuita."

Por tanto, este Registro, que conforme a la Ley se trata de un órgano integrado en la Agencia de Protección de Datos[27] , se convierte en la vía adecuada

■ 26 Art. 36 a) de la LORTAD.
■ 27 Art.38 de la Ley.

para ejercer el derecho de información. Con él queda garantizado el principio de transparencia propio de una sociedad democrática, poniendo en conocimiento de las personas de donde pueden proceder los potenciales riegos para sus derechos. Por otra al conocerse qué datos se procesan en una sociedad, quién los realiza, con qué fin, etc. se brinda a los particulares la información necesaria para después ejercitar, si así lo desea, los derechos de acceso, rectificación y cancelación[28].

De lo anterior se deduce obviamente que para que el mencionado Registro contenga tal información habrá sido necesaria la previa inscripción de todos los ficheros. Naturalmente así lo exige la LORTAD:

Artículo 38. El Registro General de Protección de Datos.

"2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros automatizados de que sean titulares las Administraciones Públicas.

b) Los ficheros automatizados de titularidad privada...

c) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación y cancelación."

Dejando de lado la modalidad de inscripción que se establece para los ficheros de titularidad privada[29], y centrándonos en los ficheros automatizados de la Administraciones Públicas, a los que se refería la pretensión del demandante, conviene realizar unas cuantas consideraciones. No obstante comenzaremos con una observación que afecta con carácter general tanto a los ficheros de titularidad pública como privada:

- Como hemos dicho, este Registro forma parte de la estructura orgánica de la Agencia de Protección Datos" cuyo Estatuto fue aprobado por el Gobier-

■ 28 Esta doble perspectiva institucional y subjetiva la pone de manifiesto. P. LUCAS MURILLO DE LA CUEVA en "La protección de los datos personales ante el uso de la informática..." (11 parte), cit., p.26.

■ 29 La LORTAD establece un mecanismo específico para poder ejercer el derecho de información con respecto a los ficheros de titularidad privada. Así el art. 24. Notificación e inscripción registral nos dice:
1. Toda persona o entidad que proceda a la creación de ficheros automatizados de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.
2. Por vía reglamentariase 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 y las cesiones de datos de carácter personal que se prevean realizar..."

no mediante decreto a primeros del mes de mayo[30]. Sin embargo, en la fecha en que se escriben estas páginas, -mediados de octubre- no se ha puesto todavía en marcha dicha Agencia y en consecuencia tampoco el Registro General de Protección de Datos[31]. El Sr. Olaverri cuando presentó su escrito, en 1986, no contaba con este sistema de Registro para hacer posible el ejercicio de sus derechos, pero tampoco parece claro que para cuando se ejecute esta sentencia haya sido creado[32]. La tardanza de la puesta en funcionamiento de este órgano imposibilita tanto la inscripción en este Registro de los ficheros de datos personales, tanto de titularidad pública como privada, creados tras la entrada en vigor de la LORTAD, como la de los ficheros anteriores existentes a este momento, los cuales conforme a la disposición adicional segunda deberían ser declarados antes del 31 de enero de 1994[33]. Como consecuencia se hace imposible el ejercicio del derecho a la información, vía Registro General de Protección de Datos, para conocer la existencia de ficheros automatizados de datos de carácter personal, sus finalidades y la identidad del responsable del fichero.

-Centrándonos en los ficheros automatizados de titularidad pública, resulta sumamente interesante detenernos en un artículo de la Ley, el dieciocho, dedicado expresamente a la creación, modificación y supresión de los ficheros de titularidad pública.

Artículo 18. Creación, modificación y supresión.

"1.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.

- 30 Real Decreto 428/1993, de 26 de marzo por el que se aprueba el Estatuto de la Agencia de Protección de Datos. Boletín Oficial del Estado, nº 106, de 4 de mayo de 1993, pp. 13244 y ss.
- 31 El Estatuto de la Agencia de Protección de Datos establecía un calendario para su puesta en funcionamiento: había que proponer una serie de miembros para componer un Consejo Consultivo, y a partir de éstos el Gobierno, a propuesta del Ministerio de Justicia, nombraría al Director, el cual, dicho sea de paso, está llamado a cumplir la mayoría de las funciones de la Agencia. La disolución de las Cortes, el pasado junio, retrasó estos plazos. Por otra parte, parecía lógico que para adoptar una decisión de esta transcendencia habría de esperarse a la formación del nuevo Gobierno. De este modo, muy recientemente según Orden de 15 de octubre de 1993 se dispone la publicación del Acuerdo del Consejo de Ministros por el que se nombran los Vocales del Consejo Consultivo de la Agencia de Protección de Datos, Boletín Oficial del Estado, nº 248, de 16 de octubre de 1993, pp. 29256 y ss. Sin embargo, falta aún por determinar el nombramiento del Director, pieza imprescindible para que comience a funcionar la Agencia.
- 32 Si se aplica para este caso el artículo 42 de la Ley 20/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, a partir de la solicitud de ejecución de la sentencia, el Gobernador Civil tendría un plazo de tres meses para comunicar esta información al Sr. Olaverri. Sería deseable que para entonces se hubiese puesto en marcha la Agencia.
- 33 Disposicional adicional segunda. Ficheros existentes con anterioridad a la entrada en vigor de la Ley.
  "1. Dentro del año siguiente a la entrada en vigor de la presente Ley Orgánica deberán ser comunicados a la Agencia de Protección de Datos los ficheros y tratamientos automatizados de datos de carácter personal existentes con anterioridad y comprendidos dentro de su ámbito de aplicación."

2. Las disposiciones de creación o de modificación de los ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero automatizado y la descripción de los tipos de datos de carácter personal.

e) Las cesiones de datos de carácter personal que, en su caso, se prevean.

f) Los órganos de la Administración responsables del fichero automatizado.

g) Los servicios o unidades ante los que pudieran ejercitarse los derechos de acceso, rectificación y cancelación...".

De la lectura de este precepto se desprende que basta con la publicación de una disposición general para crear o modificar un fichero de titularidad pública. En principio, no se exige para nada la intervención de la Agencia en este primer momento. Otra cuestión es que, sin lugar a dudas, conforme a lo preceptuado por la Ley y el Estatuto de la Agencia estos ficheros deban de ser inscritos. En consecuencia cabría deducir que, a pesar de la situación actual en la que no se ha puesto en marcha la Agencia de Protección de Datos, ni en consecuencia el Registro, cualquier persona, mediante la consulta al Boletín Oficial del Estado o al diario oficial correspondiente, podría saber quién es el responsable, el domicilio, los fines -en definitiva, todos los datos necesarios para ejercitar el derecho de acceso, rectificación y cancelación- de todos los ficheros que se vayan , creando, o modificando. Además esta facultad no sólo existe para los nuevos ficheros sino que ha de entenderse que se debería extender también a los ficheros existentes con anterioridad a la entrada en vigor de la Ley, pues, conforme a la disposición adicional segunda "los ficheros automatizados de las Administraciones Públicas deberán adoptar una disposición de regulación del fichero o adaptar la que existiera". Esta adopción o adaptación de disposiciones debe interpretarse como una remisión a lo preceptuado por el artículo 18.

Esta interpretación, que posibilitaría el derecho de información en la actualidad, presenta, sin embargo, ciertas dificultades.

- Para comenzar hay que decir que se trataría de un ejercicio "parcial" del derecho de información. El derecho de información concebido como el derecho público a conocer la existencia de todos los ficheros automatizados se ejerce realmente a través del Registro General de Protección de Datos. Cuando el mismo entre en funcionamiento y cuando se inscriban todos los ficheros automatizados de titularidad pública anteriores a la entrada en vigor de la LORTAD y se vayan inscribiendo los de nueva creación así como las diversas modificaciones, el listado que de los mismos se publique si será realmente una garantía, una expresión del principio de transparencia para conocer "todos" los tratamientos automatizados que en manos de las Administraciones Públicas existen en ese momento en la sociedad española. Por tanto el ejercicio del derecho de información que ofrece la correlativa disposición general creadora de un fichero es un ejercicio parcial de este derecho, ya que solamente se irá conociendo en la medida en que se vayan publicando los ficheros en los Boletín o diarios oficiales y no se configura como la facultad de ver en su conjunto los tratamientos automatizados existentes en cada momento en el país.

- Hasta la fecha en que escribimos -17 de octubre- no ha sido publicada ninguna disposición general creadora o modificadora de fichero automatizado cuyo titular sean las Administraciones Públicas. Esto no quiere decir que en un futuro y antes de la entrada en funcionamiento del Registro General de Protección de Datos, si así se desea, no se vayan comenzando a publicar, pero, también es cierto, y dando por supuesto la complejidad que para ciertos ficheros automatizados anteriores supone la adaptación a lo establecido en la LORTAD, que si esta fuera la voluntad, nueve meses desde la entrada en vigor de la Ley es tiempo suficiente para poderlo haber llevado a cabo. En el fondo de todo esto quizás esté presente otra cuestión, a saber, la necesidad, a pesar de que explícitamente no se mencione en el artículo 18, de informe previo de la Agencia de Protección de Datos para poder crear o modificar un fichero de titularidad pública.

Así, la Exposición de Motivos de la LORTAD dice:

" ...Con la pretensión de evitar una perniciosa burocratización, la Ley ha desechado el establecimiento de supuestos como la autorización previa o la inscripción constitutiva en un registro. Simultáneamente, ha establecido regímenes diferenciados para los ficheros en razón de su titularidad, toda vez que, con toda evidencia, resulta más problemático el control de los de titularidad privada que el de aquéllos de titularidad pública. En efecto, en lo relativo a estos últimos, no basta la mera voluntad del responsable del fichero sino que es precisa norma habilitante, naturalmente pública y sometida al control jurisdiccional, para crearlos y explotarlos, siendo en estos supuestos el informe

previo del órgano de tutela el cauce idóneo para controlar la adecuación de la explotación a las exigencias legales y recomendar, en su caso las medidas pertinentes".

Referencia, por tanto, al informe previo de la Agencia de Protección de Datos.

En este sentido el artículo 36 de la Ley establece que:

"Son funciones de la Agencia de Protección de Datos:

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley".

Sobre este particular, LUCAS MURILLO DE LA CUEVA[34] sostiene que, en efecto, el acto normativo de creación de un fichero público es una disposición general y por tanto en principio nos encontraríamos en la hipótesis del artículo 36.h): necesidad de informe previo de la Agencia. Pero, sin embargo, la creación, (o en su caso modificación) de un fichero no es una disposición general que desarrolle la LORTAD sino que se trata de un acto de aplicación de la Ley y este supuesto no se contempla en el mencionado precepto.

Sin embargo la no existencia de una definición jurídico-positiva de lo que se deba entender por desarrollo, unido a la mayor garantía que supondría la intervención de la Agencia para controlar que estas disposiciones adopten (o en su caso se adapten) una (a la) regulación legal, permitiría extender también para este supuesto,-conforme a una interpretación amplia del artículo 36.h)-, la exigencia del informe previo.

Por otra parte, en su opinión, el artículo 5 del Estatuto de la Agencia de Protección de Datos (en adelante EAPD) dedicado a la función consultiva de la Agencia abre un resquicio para una interpretación diferente, no centrada en este caso en una interpretación amplia del término "desarrollo", pero con igual consecuencia. Así, conforme a este precepto, junto al informe preceptivo de los proyectos de disposiciones generales de desarrollo de la Ley, el apartado b) establece igualmente este informe preceptivo para cualesquiera proyectos de ley o de reglamentos que incidan en la materia propia de la Ley Orgánica 5/1992. De este modo se puede negar que la creación de un fichero sea desa-

■ 34 Vid. P. LUCAS MURILLO DE LA CUEVA, "La protección de los datos personales ante el uso de la informática" (II parte), cit., 37, p.95.

rrollo de la LORTAD pero no puede decirse que este mismo acto no incide en la materia propia de dicho texto legal[35] .

Desde nuestro punto de vista, si bien el informe previo preceptivo sería un cauce sumamente interesante para la creación de estos ficheros, y así además lo demuestra la exigencia del mismo en otras legislaciones de protección de datos de nuestro entorno más próximo[36], no parece tan evidente que del texto de la Ley ni del EAPD se puedan extraer, al menos nítidamente, la solución que ofrece el profesor LUCAS MURILLO DE LA CUEVA. El apartado b) del artículo 5 del Estatuto cuando se refiere a proyectos de ley o de reglamentos que incidan en la materia propia de la LORTAD está pensando en otro tipo de disposiciones como puèdan ser leyes o reglamentos sectoriales (leyes relativas a secreto estadístico o información médica, tributaria, etc). Por su parte el silencio que a este respecto guarda el artículo 18 de la Ley y la interpretación un tanto forzada del apartado h) del artículo 36 con respecto a lo que se deba de entender por "desarrollo de la LORTAD" nos hace dudar de la exigencia de la necesidad de la intervención de la Agencia antes de la publicación de estos ficheros en el Boletín o diarios oficiales en la creación (o modificación) de ficheros de titularidad pública.

Dependiendo de la solución que en su día se determine podrá ocurrir que hasta que no se produzca la puesta en marcha de la Agencia, no se podrá ejercitar -aunque sea como dijimos de una manera "parcial"- el derecho de información, -en el supuesto de que el informe previo de la Agencia sea preceptivo-, o por el contrario a pesar de la no entrada en funcionamiento de la misma gracias a la publicación de estas disposiciones generales en el Boletín o diarios oficiales se podrá ir conociendo aunque sea paulatinamente informaciones de los ficheros que se vayan creando o adaptando, (identidad del responsable, domicilio, categoría de destinatarios, fines, etc) las cuales forman parte del derecho de información.

Lo cierto es que la publicación oficial de estas disposiciones generales ofrece no sólo en el momento actual, -si tales disposiciones fueran publicadas antes de la puesta funcionamiento del Registro- sino también hacia futuro -cuando el citado órgano de la Agencia haya sido puesto en marcha- la posibili-

■ 35 Esta nueva interpretación que ofrece el EAPD la recoge el autor en su obra más reciente. Vid P. LUCAS MURILLO DE LA CUEVA, "Informática y Protección de datos personales..." cit, nota 118, p.93.

■ 36 Así el artículo 15 de la Ley Francesa n°78-17, de 6 de enero de 1978, sobre Informática, ficheros y libertades exige el previo dictamen motivado de la Comisión Nacional de Informática y de las Libertades para los tratamientos de informaciones nominativas efectuados por cuenta del Estado, de un organismo público o de una entidad territorial, o de alguna persona jurídica de derecho privado.

dad de que el lector del BOE o en su caso de los diarios oficiales (si bien una escasa minoría del país) conozca con anterioridad a la inscripción en el Registro, toda la información necesaria para ejercitar los derechos de acceso, rectificación y cancelación[37]. En cualquier caso se ha de reseñar que estas conclusiones, en lo que respecta a la posibilidad de ejercicio de estos últimos derechos, deben ser relativizadas.

El derecho de información, sea cual sea el momento, (sin o con órgano de tutela) nunca debe ser una condición previa para el ejercicio del derecho individual a conocer o derecho de acceso. En consecuencia, no hace falta el que se sepa que un fichero existe, basta con que exista para que sea accesible[38]. Ahora bien, en estos momentos transitorios antes de la puesta en funcionamiento de la Agencia, -concretamente del Registro General- y si fuera factible publicar las mencionadas disposiciones sin necesidad de intervención de la misma, la información que se obtiene de la consulta a los boletines o diarios oficiales podría servir, -especialmente con respecto a los ficheros anteriores a la Ley (pues como veremos más tarde el conocimiento de los datos los ficheros de nueva creación se puede obtener por otras vías)- para conocer, además de qué ficheros existen, quién es el responsable, qué fines se persiguen con los mismos, etc -manifestaciones por otro parte interesantes del derecho de información-, en qué tipo de ficheros estamos registrados. Este tipo de información hasta el momento actual no era posible saberse en España, pero la disposición general creadora del fichero la facilita al establecerse que ésta deberá indicar "las personas o colectivos sobre los que pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos".

Como ya se ha puesto de manifiesto, además de esta vía, -la publicación en boletín o diarios oficiales de las disposiciones relativas a ficheros de titularidad pública- hay que decir que el mecanismo adecuado para ejercitar el derecho de información, cuando se ponga en marcha, será el Registro General de Protección de Datos. Su consulta será pública y gratuita y por tanto se ha de entender que este derecho se puede ejercer cuantas veces se quiera. Corresponde al Registro y a la Agencia "velar por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación". Esta publicidad, a mi entender debe ser entendida en el sentido más

■ 37 Esta circunstancia relativa a la posibilidad de conocer desde el primer momento la información de cada fichero automatizado de titularidad pública, también ha sido puesto de manifiesto por P. LUCAS MURILLO DE LA CUEVA, "Informática y Protección de datos personales...", cit., p.94.

■ 38 HERNANDO COLLAZOS, "La Comunidad Económica Europea y la Informática..." cit., p 87.

amplio posible. La Ley y el EAPD se refieren únicamente a la publicación y difusión anual de un catálogo que contenga la relación de los ficheros automatizados inscritos en el Registro[39]. Pero, para ello, habrá que esperar un año desde que comience a funcionar la Agencia y además y posteriormente para que este listado sea conocido por el número máximo de personas habrá que darle una buena difusión. Lo más acertado es que desde el primer momento en que se vayan inscribiendo los ficheros automatizados pudieran ser conocidos. Así además de la consulta al Registro, sería sumamente interesante que se arbitraran medidas -como se viene realizando en países vecinos- a las cuales se podría hacer referencia, por ejemplo, en el reglamento que en su día desarrolle el derecho de acceso[40] tales como la difusión del listado de los ficheros que existan y que se vayan creando en publicidad oficial en ayuntamientos, prensa local, etc[41] .

En cuanto a la consulta al Registro o a la Agencia también resulta ilustrativo el ejemplo francés, donde la lista de los tratamientos automatizados, (además de otras cuestiones, como puedan ser las recomendaciones o decisiones de la institución de control, o la información sobre los derechos de la persona, etc) pueden ser accesibles por un servicio telemático de información[42].

La adopción de medidas como estas conseguiría materializar el derecho de información pues tanto la LORTAD como el EAPD insisten reiteradamente además de, en la necesidad de velar por la publicidad de los ficheros automati-

- 39 El art. 36 de la LORTAD establece que: "Son funciones de la Agencia de Protección de Datos:
  j)Velar por la publicidad de la existencia de los ficheros automatizados de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine". Por su parte, el art.7 del EAPD denominado Publicidad de los ficheros automatizados" especifica que se tratará de un catálogo anual de los ficheros inscritos en el Registro General.
- 40 El artículo 16 de la Ley establece que el procedimiento para ejercitar el derecho de acceso, será establecido reglamentariamente.
- 41 A estas medidas y a otras más se refiere la deliberación n°80-10 del 1 de abril de 1980 de la Comisión Nacional de Informática y Libertades francesa (C.N.I.L.) que adopta una recomendación relativa a la puesta en funcionamiento del derecho individual al acceso a los ficheros automatizados. (J.O. de 29 de mayo de 1980). Este texto se encuentra recogido en la obra de J. FRAYSSINET "Informatique, fichiers et libertés". Ed. Litec, pp. 211 yss.
- 42 El servicio telemático de información (Minitel 3615, código CNIL) es accesible desde el 2 de abril de 1990. Funciona 24 horas al día e informa de diversas cuestiones como las arriba apuntadas y de otras más, por ejemplo: funciones de la CNIL, el sistema para la declaración de los tratamientos, flashes de actualidad, etc. El número mensual medio de conexiones es superior a 600 y el tiempo medio de una consulta es del orden de 6 minutos. De todo ello se da cuenta en el "11e Rapport de la Commission Nationale de l'informatique et des libertés 1990". C.N.I.L., La documentation française, París, 1991, p.94. Por otra parte, la propia Ley 20/1992, de 26 de noviembre, del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común establece en su artículo
  45.2: "Cuando sea compatible con los medios técnicos de que dispongan las Administraciones Públicas, los ciudadanos podrán relacionarse con ellas para ejercer sus derechos a través de técnicas y medios electrónicos, informáticos o telemáticos con respeto de las garantías y requisitos previstos en cada procedimiento".

zados, en la de "informar a las personas de los derechos que la Ley les reconoce en relación con el tratamiento automatizado de sus datos"[43]. Para ello, para difundir esta información, se establece que la Agencia podrá promover campañas de difusión, valiéndose de los medios de comunicación social .

Estas campañas de difusión son decisivas para que los ciudadanos conozcan sus derechos, sobre todo en el momento actual que existe un profundo desconocimiento sobre esta materia. Por lo tanto, esta actividad de difusión debería estar formulada como una obligación de la Agencia y no como una mera posibilidad[44]. Por otra parte, si se llevara a la práctica, se debería informar asimismo de cómo han de ejercitarse estos derechos. En relación por ejemplo del derecho que hemos estudiado, el derecho de información, se habrá de mencionar todas las vías existentes para el ejercicio del mismo. Así la consulta al Registro -con todas las formas posibles que se adopten para su conocimiento, consulta oral, escrita, por vía telemática, etc-, la posibilidad de consultar o informarse del listado de los ficheros existentes y de los que se vayan creando (o modificando) por los medios que se establezcan (Boletín o diarios oficiales, publicidad en lugares oficiales, prensa..) y la difusión del catálogo anual de ficheros y de la memoria anual que publique la Agencia (p.e distribución en el seno de la Administración y de las empresas privadas). Para todo ello habría que reservar ciertos espacios en la radio, televisión, prensa, etc y no estaría de más la publicación, a modo de guía, de todas estas cuestiones.

Hechas todas estas consideraciones sobre el derecho de información, (con especial relación a los ficheros de titularidad pública), a los instrumentos para ejercitar este derecho en la situación actual antes de la entrada en funcionamiento de la Agencia -y del Registro-, y a los mecanismos que garantizarían un mejor conocimiento y práctica del mismo, volvamos a los términos en que debe ser interpretado el fallo de la sentencia del Tribunal Constitucional anteriormente estudiada.

Con respecto al derecho de información el TC reconoce al actor el derecho a que el Gobernador Civil le comunique la existencia de los ficheros automatizados de datos de carácter personal, dependientes de la Administración Civil del Estado, las finalidades de estos ficheros, y la identidad y el domicilio

- 43 Art. 36 e) de la ley y art. 4 del EAPD. En este sentido, la CLI entre sus propuestas de enmienda al Anteproyecto de Real Decreto de Estatuto de la Agencia de Protección de Datos proponía la creación de una Oficina de Información y Asesoramiento en el órgano de la Agencia encargado de atender las peticiones de información y asesoramiento que ésta recibiera por parte de los ciudadanos, empresas u organizaciones en relación con la Agencia o la aplicación de la LORTAD.
- 44 Art. 4 del EAPD. La CLI en relación con el estatuto formulaba un cambio de redacción en vez de la Agencia de Protección de Datos "podrá" la Agencia de Protección de Datos "deberá".

de cada una de la autoridades responsables de los mismos. Previamente en este mismo fundamento jurídico, el noveno, expone que:

"La creación del Registro General de Protección de Datos, y el establecimiento de la Agencia de Protección de Datos, facilitarán y garantizarán el ejercicio de los derechos de información y acceso de los ciudadanos a los ficheros de titularidad pública, y además extienden su alcance a los ficheros de titularidad privada. Pero ello no desvirtúa el fundamento constitucional de tales derechos, en cuanto imprescindibles para proteger el derecho fundamental a la intimidad en relación con los ficheros automatizados que dependen de los poderes públicos. *Ni tampoco exonera a las autoridades administrativas* del deber de respetar ese derecho de los ciudadanos, al formar y utilizar los ficheros que albergan datos personales de éstos, *ni del deber de satisfacer las peticiones de información deducidas por las personas físicas en el círculo de las competencias propias de tales autoridades.*"[45]

Del texto anterior cabe deducir la siguiente conclusión:

- Tanto en ausencia de desarrollo legislativo del art. 18.4 CE, (situación en la que se encontraba el demandante en 1986), como tras la entrada en vigor de la LORTAD pero sin producirse la puesta en funcionamiento del Registro y de la Agencia General de Protección de Datos (situación en la que se produce la sentencia) o como tras su "creación" y "establecimiento" (situación futura), las autoridades administrativas deberán satisfacer las peticiones de información que les soliciten las personas físicas, si bien en el círculo de sus competencias.

El derecho de información, como hemos venido afirmando, presupone que se conozcan qué ficheros automatizados existen en esa sociedad, quién es el responsable de los mismos, qué fines, qué personas o colectivos, ante qué servicios se debe ejercitar, etc. La vía que en España se ha adoptado para posibilitar el ejercicio de este derecho es la inscripción de estos ficheros automatizados con todos esos extremos en un Registro Público. Evidentemente, y si cuando se ponga en funcionamiento se realiza de forma correcta, no hay ningún problema para que cualquier autoridad administrativa controla al día toda esta información, -incluso por consulta telemática al Registro-, sin embargo a falta de la puesta en funcionamiento del mismo la obtención de esta información puede ofrecer dificultades. Así, en opinión del Abogado del Estado:

"Parece obvio que la petición se dirigió al Gobernador Civil como representante permanente del Gobierno de la Nación en la provincia, pero es igual-

■ 45 El subrayado es nuestro.

mente evidente que carecía de los medios precisos para poder satisfacer la prestación informativa que se le recababa. Cada uno de los ficheros tienen sus propias y específicas normas, por no hablar de los ficheros de índole tributaria... la información sólo se hubiera podido suministrar si se hubiera producido una intervención legislativa previa, que hubiera organizado las garantías complementarias previstas en el art. 8 del Convenio europeo de 1981."(Antecedente sexto).

Por tanto, conforme a esto, en ausencia de desarrollo legislativo, como era la situación en 1986, no se podría obtener del Gobernador Civil satisfacción a esta pretensión. En la época actual la entrada en vigor de la LORTAD podría permitir al mismo un mejor conocimiento de los ficheros automatizados de las Administraciones Públicas, si como pusimos de relieve, a pesar de la no intervención de la Agencia estos nuevos ficheros se fueran creando y los anteriores a la Ley adaptando o adoptando por medio de las correspondientes disposiciones generales. Sea como fuere y en cualquier caso seguiría faltando el mecanismo adecuado, el funcionamiento del Registro General, para el correcto ejercicio del derecho de información.

Sin embargo, el TC opina -como hemos visto anteriormente- que el Gobernador Civil, cuando el actor lo solicitó en 1986, debería haber satisfecho esta demanda y por supuesto, tampoco, en la actualidad nada impide que el Gobernador satisfaga esta pretensión.

"El que un determinado órgano administrativo disponga, o carezca, de los medios materiales o de las atribuciones competenciales precisos no sirve para discernir los derechos de un ciudadano, especialmente si esos derechos son declarados por la Constitución. La cuestión que debemos determinar en este proceso es si el actor tenía o no derecho, en virtud del art.18 CE, a que la Administración le suministrase la información que solicitaba. Si tiene derecho a ella, es deber de todos los poderes públicos poner los medios organizativos y materiales necesarios para procurársela.."(fundamento jurídico tercero).

En consecuencia, para el TC la ausencia de medios organizativos, cuando el actor presentó su solicitud, o en este momento debido al retraso en la puesta en funcionamiento de la Agencia y del Registro, no exonera al Gobernador Civil de si existe este derecho de información, este derecho a conocer la existencia de los ficheros automatizados, poner todos los medios posibles para conseguirle esta información. El que la creación del Registro facilite el ejercicio de este derecho no significa que mientras éste no se ponga en funcionamiento

no se deban satisfacer las peticiones de información, aunque resulte más dificultoso llevarlo a cabo[46].

Por tanto el Sr. Olaverri podrá obtener del Gobernador Civil de Guipúzcoa esta información en breve plazo desde el momento en que se solicite la ejecución de la sentencia[47].

No creo que imitando la demanda estudiada abunden solicitudes, antes de que comience a funcionar el Registro General, requiriendo a cualquier órgano de la Administración el derecho a conocer la existencia de ficheros automatizados públicos. Pero si así fuera las Administraciones deberían poner todos los medios para satisfacer estas peticiones. Desde luego, la mayor dificultad estribaría en conseguir adecuadamente toda esta información: relación de ficheros, identidad y domicilio de responsables, fines, etc. Por otra parte, hasta que no comience a funcionar el Registro General no se podrá, dado el caso y si fueran numerosas las solicitudes de derecho de información dirigidas a una Administración concreta con el fin de evitar colapsos, remitir las mismas al mencionado órgano de la Agencia[48].

Para terminar una última observación. El demandante solicitó información sobre los ficheros automatizados de la Administración del Estado o cualquier organismo de ella dependiente pero como es lógico, conforme al ámbito de sus competencias el Gobernador Civil sólamente le podrá dar información de los ficheros de la Administración Civil del Estado, quedando por tanto excluida la Administración Militar[49]. Por otra parte, tampoco le dará la información relativa a los ficheros de las Comunidades Autónomas y de sus Territorios Históricos. No obstante, cuando entre en funcionamiento el Registro General de Protección de Datos, éstos también deberán inscribirse en el mismo

- 46 Al menos actualmente conforme al artículo 18 y la disposición adicional segunda los ficheros automatizados de titularidad pública estarán a punto de adoptar una disposición de regulación o de adaptar la ya existente.
- 47 Como hemos puesto de manifiesto en la nota n° 30,de aplicarse para este caso el artículo 42 de la Ley 20/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en un plazo de tres meses.
- 48 Con respecto a este derecho de información, la respuesta por el Registro de las solicitudes de información que la Administración le remitiera cumpliría perfectamente "el deber de satisfacción a las peticiones de información "por las autoridades administrativas a la que alude el TC en esta sentencia.
- 49 En Francia, por ejemplo, el Consejo de Estado puede establecer que los actos reglamentarios relativos aciertos tratamientos relativos a la seguridad del Estado, la defensa o la seguridad pública no sean publicados (art 20 de la Ley Francesa n°78-17, de 6 de enero de 1978, sobre Informática, ficheros y libertades), y por tanto las personas sobre estos tratamientos no sepan que existen, quién es el responsable, los fines, etc. Es decir se les niega en relación a los mismos el derecho de información (aunque después, como hemos comentado en nota 25, por medio de la CNIL, se pueda ejercitar el derecho de acceso). La LORTAD no dice nada sobre este tema. En consecuencia sería deseable que al menos se supieran estas informaciones independientemente que después con respecto a este tipo de ficheros la Ley establezca que el derecho de acceso no es o es difícilmente posible.

según especifica el art. 24 del EAPD. De esta manera podrán ser conocidos, sin perjuicio de que si así lo desean las Comunidades Autónomas puedan crear sus propios registros públicos en el ámbito de sus competencias (art. 40.2 de la LORTAD).

En relación con el derecho de acceso, conviene distinguir, como se hizo en páginas anteriores:

a) El derecho del individuo a conocer la existencia de información que le concierne en un fichero determinado.

b) El derecho del individuo a conocer el contenido de la información que le concierne en un fichero determinado.

Mientras que el artículo 8 b) del Convenio 108 se refería expresamente a estos dos aspectos -"la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernen a dicha persona, así como la comunicación de dichos datos de forma inteligible"- el legislador español ha optado por no hacer alusión expresa a los mismos, aunque se ha de entender que la redacción genérica del artículo 14 de la LORTAD garantiza ambos derechos:

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

Sin lugar a dudas, la solicitud y obtención de información se puede referir tanto a la existencia o a la ausencia de datos que le afectan como al contenido de los mismos.

Así, y con respecto al derecho a conocer si existen datos referidos a una persona determinada en los ficheros automatizados hay que distinguir la situación de los ficheros previos y la de los posteriores a la entrada en vigor de la LORTAD.

En este sentido el artículo 5 de la Ley denominado "derecho de la información en la recogida de los datos" establece la obligación de informar de modo expreso, preciso e inequívoco a quien se solicite datos personales de la existencia del fichero automatizado, la finalidad de la recogida de los datos y los destinatarios de la información, el carácter obligatorio o facultativo de la respuesta, las consecuencias de la obtención de los datos o de la negativa a suministrarlos, la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, y de la identidad y dirección del responsable del fichero.

Por tanto, en relación a los ficheros posteriores a la Ley, (o ficheros anteriores a la misma pero que soliciten de nuevo datos personales) las personas podrán conocer en qué ficheros están registrados, qué tipo de datos se registran y quién es el responsable de ficheros si se quiere ejercitar posteriormente sus derechos.

Hace siete años cuando el Sr. Olaverri dirigió su solicitud al Gobernador Civil, el actor desconocía qué ficheros existían, en cuáles se encontraba registrado y qué datos de él constaban en los mismos. En el momento actual, exceptuando la situación de los ficheros que se creen tras la entrada en vigor de la Ley o de los anteriores a la misma pero que soliciten nuevamente datos personales al titular de los datos que quiera saber si está o no incluido en los distintos ficheros automatizados y qué datos de él se contienen no le quedará más remedio que dirigirse y acceder a todos los posibles ficheros[50].

Según tuvimos ocasión de comprobar, en un futuro próximo, la entrada en funcionamiento del Registro General de Protección de Datos puede, en parte, facilitar esta labor. Así a pesar de que de este órgano sólo se podrá conocer el listado de los ficheros existentes, pero no si un determinado fichero contiene datos nuestros y en qué sentido, el EAPD establece que en los asientos de inscripción de los ficheros de titularidad pública habrá de figurar toda la información contenida en la disposición general de creación o modificación del fichero[51]. Como tuvimos ocasión de ver, una de estas informaciones es la relativa a "las personas o colectivos sobre los que pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos". Por lo tanto, si no nos encontramos en el supuesto del artículo 5 y por tanto no conocemos en qué ficheros estamos registrados, esta información mencionada puede servir a modo de orientación para el posterior ejercicio del derecho de acceso[52].

En cualquier caso se ha de decir que la solución más adecuada consistiría en informar a los afectados en qué ficheros anteriores a la entrada en vigor de la LORTAD se encuentran registrados, y qué datos de cada uno constan en cada uno de ellos. Sin embargo, la disposición adicional segunda que se ocupa

- 50 M. LOPEZ-MUNIZ GONI critica lo anómalo de esta situación en "Jornadas Abogacía e Informática...", cit., p. 92.
- 51 Art. 24.2 del EAPD: "En los asientos de inscripción de los ficheros de titularidad pública figurará, en todo caso, la información contenida en la disposición general de creación o modificación del fichero, de conformidad con lo previsto en el artículo 18.2 de la Ley Orgánica 5/1992, de 29 de octubre.
- 52 Cuando hablamos del derecho de información se hizo referencia a que si se publicarán estas disposiciones sin necesidad de intervención de la Agencia en estos momentos transitorios antes de la puesta en funcionamiento de la misma ,-concretamente del Registro General- esta misma información acerca de las personas o colectivos sobre los que pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos" le serviría de ayuda a quien siguiera la publicación de las misma en el Boletín o diarios oficiales para saber a qué ficheros determinados le interesa dirigirse.

de los ficheros que existían previamente a la Ley silencia por completo esta cuestión[53].

Además por otra parte, las numerosas excepciones con las que cuenta la Ley hará muy difícil incluso con respecto a los ficheros posteriores a la Ley (o a ficheros anteriores que entren dentro del supuesto del artículo 5) conocer a una persona con precisión en todos y cada uno de los ficheros en que se encuentra. Así toda la información a la que se alude en este precepto podrá ser obviada según el apartado 3 del mencionado artículo 5 "si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban" o "si la información al afectado impida o dificulte gravemente el cumplimiento 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 las infracciones penales y administrativas". (art. 22). Además del sistema de cesiones de datos, en el que en determinados casos no es necesario el consentimiento del afectado y por tanto el titular pierde el control de dónde y cómo se registran los datos que él un día dió.

Visto el régimen que la LORTAD establece, si bien podrá haber un mayor conocimiento acerca de en qué ficheros de nueva creación nos encontramos y qué datos se contienen, en relación a los ficheros anteriores a la Ley, la certeza no es ni mucho menos absoluta sobre todo en lo que se refiere a los ficheros de titularidad pública.

Por todo ello, se hace necesario que el ejercicio del derecho de acceso, cuyo procedimiento queda remitido a la vía reglamentaria, se regule de la manera más flexible en la medida de las posibilidades.

Así nada debe de impedir que dicho derecho se ejercite:

- solicitando que se le informe si en determinado fichero constan o no datos que le conciernan y que esta información sean comunicada.

- pidiendo ante el responsable de fichero si en sus registros consta información sobre él y en caso positivo se le comunique toda ella.

■ 53 La disposición adicional segunda establece: 1. Dentro del año siguiente a la entrada en vigor de la presente Ley Orgánica deberán ser comunicados a la Agencia de Protección de Datos los ficheros y tratamientos automatizados de datos de carácter personal existentes con anterioridad y comprendidos dentro de su ámbito de aplicación". Esta comunicación a la Agencia de Protección de Datos de todos estos ficheros automatizados está pensando en la inscripción de los mismos, y no creo, aunque fuera deseable, que posteriormente, la Agencia o los responsables de los ficheros notifiquen a los afectados en qué ficheros se encuentran, y menos aún qué datos de ellos se contienen.

Para la primera opción hay que conocer la existencia de un fichero determinado, información difícil de saber si previamente no se conocen qué ficheros existen. Ya vimos las posibilidades que la LORTAD establece para el conocimiento de los mismos (consulta al Registro, publicación Boletín o diarios oficiales para los ficheros de titularidad pública, catalogo anual de ficheros inscritos..) y las medidas que para facilitar el derecho de información se podrían arbitrar (publicidad en ayuntamientos, prensa, acceso telemático, campañas de difusión...)[54] y por tanto nos remitimos a lo que anteriormente se ha dicho. Simplemente poner de relieve que esta forma de ejercicio resulta prácticamente imposible para el demandante en 1986, y bastante difícil en el momento transitorio en el que nos encontramos antes de la puesta en funcionamiento del Registro (a no ser que conforme al artículo 5 se estuvieran ya solicitando datos y se informara en qué fichero van a quedar registrados y quién es el responsable de los mismos)[55] .

La segunda opción, y centrándonos en los ficheros de titularidad pública, es la que adopta el Tribunal Constitucional en esta sentencia pues reconoce el derecho de acceso del Sr. Olaverri a todos los ficheros sobre los que ostente competencia el Gobernador Civil.

Hasta que no se sepa con mayor precisión qué ficheros automatizados existen ni tan siquiera quién responde de ellos ni en el caso de los ficheros de titularidad publica ante qué servicios o unidades administrativas se pueden ejercitar estos derechos, lo más lógico es que quien deseara ejercitar este derecho se dirigiera a la Administración pidiendo que se le comunique los datos que a él le conciernen de todos los ficheros automatizados sobre los que ostente competencia. Pero también posteriormente, cuando entre en funcionamiento la institución de control, como hemos advertido, debido al régimen de excepciones que establece en la Ley, puede resultar sumamente interesante el dirigirse a un órgano o autoridad de la Administración para que nos comunique toda la información que sobre nosotros exista en todos sus ficheros automatizados.

Por otra parte, de las palabras del propio Tribunal Constitucional se deduce que siempre en cualquier momento: en ausencia de desarrollo legislativo, tras la entrada en vigor de la LORTAD, ya aunque se haya "creado" el Registro General o "establecido" la Agencia de Protección de Datos las autoridades administrativas deberán de satisfacer las peticiones de información que

■ 54 Así como las dificultades para ejercitar este derecho mientras no se ponga en funcionamiento el Registro General de Protección de Datos.

■ 55 0 la posibilidad mencionada de que se estuvieran publicando ya en el Boletín o diarios oficiales las disposiciones generales creadoras o modificadoras de ficheros de titularidad pública.

se les soliciten en el ámbito de sus competencias. Por tanto esta segunda modalidad de derecho de acceso también debería quedar garantizada, en opinión del Constitucional. También la propia redacción del artículo 14 de la LORTAD "derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados" permite amparar una petición de información de forma generalizada ante el responsable de fichero.

Una precisión debe ser realizada. El responsable del fichero será el órgano de la Administración que como su nombre indica "responde", pero la solicitud de derecho de acceso debe ser dirigida en el caso de los ficheros de titularidad pública a los servicios o unidades que figure en la disposición general creadora o modificadora del fichero en cuestión. Hasta que no se ponga en marcha el Registro sería difícil que se pudiera conocer este dato, e incluso podría ocurrir que no se haya asignado todavía este servicio, no obstante la Administración deberá responder. Es más a pesar de que tal información pudiera ser conocida -incluso cuando se inscriban dichos ficheros- pero el solicitante no supiera este dato, no debería haber inconveniente para que éste presentara su solicitud en la sede de la Administración correspondiente y gracias a la propia organización interna se encaminará la demanda ante el servicio o unidad competente. En este sentido, aunque sea conveniente arbitrar medidas -a las que ya aludimos- para que el solicitante sepa a quién dirigirse (vía Registro, publicidad en lugares oficiales, etc) las informaciones que contienen los ficheros públicos deben ser accesibles, si la Ley lo permite, aunque previamente no se haya ejercitado el derecho de información o no se conociese exactamente la información para dirigirse a un fichero[56] .

Otras cuestiones relativas al derecho de acceso, también están presentes en este recurso de amparo. Así el TC hace alusión, coincidiendo con lo expuesto en la demanda del solicitante y con el art. 8 b) del Convenio 108 a que el Gobernador Civil le comunique al Sr. Olaverri la información solicitada "sin demora" y "en forma inteligible".

En cuanto a la comunicación "sin demora", es interesante que el Constitucional lo recuerde. El problema consiste en determinar cuál será el plazo

■ 56 Por su parte, el artículo 37 de la Ley 20/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común establece con respecto al derecho de acceso a los archivos administrativos que éste "será ejercido por los particulares de forma que no se vea afectada la eficacia del funcionamiento de los servicios públicos debiéndose, a tal fin, formular petición individualizada de los documentos que se desee consultar, sin que quepa, salvo para su consideración con carácter potestativo, formular solicitud genérica sobre una materia o conjunto de materias". El ámbito de este derecho de acceso y al que nos referimos es diferente pero el precepto mencionado puede tener un valor orientativo. Asimismo la Deliberación -ya citada- n°80- 10 del 1 de abril de 1980 de la C.N.I.L.que adopta una recomendación relativa a la puesta en funcionamiento del derecho individual de acceso a los ficheros automatizados recuerda que la CNIL podrá acordar, a instancia del responsable de fichero, que no sean tomadas en consideración ciertas solicitudes manifiestamente abusivas por su número, su carácter repetitivo o sistemático.

razonable. Ante el silencio de la LORTAD al respecto, sin lugar a dudas esta será una de las cuestiones que habrá de resolver el reglamento que desarrolle el ejercicio de este derecho[57]. Por su parte, la Ley sí alude expresamente a la comunicación de la información en "forma inteligible", admitiendo en cualquier caso una gran variedad de formas. Así según el párrafo 2º del artículo 14:

"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 intelegible, sin utilizar claves o códigos convencionales que requieran el uso de dispositivos mecánicos específicos"[58].

Para terminar, como el propio TC expone, "el reconocimiento de estos derechos derivados del art. 18 CE, no obsta a que la autoridad administrativa deniegue, mediante resolución motivada, algún extremo de la información solicitada, siempre que dicha negativa se encuentre justificada por alguna excepción prevista por la Ley, incluido el propio Convenio de 1981". En este sentido, la LORTAD contempla una serie de supuestos conforme a los cuales el derecho de acceso puede quedar exceptuado:

Artículo 21. Excepciones a los derechos de acceso, rectificación y cancelación:

" Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior[59] podrán denegar el acceso, la rectificación o la cancelación en función de los peligros que puedan derivarse para la defensa del Estado o la seguridad pública, la protección de los dere-

■ 57 El art. 14.4 de la Propuesta modificada de Directiva Comunitaria dice que los Estados miembros reconocerán al interesado el derecho a "obtener, previa petición, con una frecuencia razonable, sin esperas ni gastos excesivos, la confirmación de la existencia o inexistencia de datos personales. . .así como, en su caso, la comunicación de esos datos...en forma inteligible;". También la mencionada Deliberación francesa relativa al derecho individual de acceso dice que la respuesta debe ser comunicada en "breve plazo", si bien regula algunas excepciones el plazo para contestar nunca podrá superar los tres meses.

■ 58 Además de estas cuestiones, el párrafo 3º de este mismo artículo hace referencia a la frecuencia en el ejercicio del derecho de acceso. De este modo será posible hacer uso de esta facultad "a intervalos no inferiores a doce meses, salvo que el afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes". En opinión de M. DAVARA RODRIGUEZ hubiese sido preferible no limitar este plazo tan categóricamente, sino que se hubiese podido ejercitar las veces que se quisiera, sin la rigidez de "acreditación" de interés legítimo. Vid al citado autor en "La ley española de protección de datos (LORTAD): ¿una limitación del uso de la informática para garantizar la intimidad?(I)" en Actualidad Jurídica Aranzadi, de 19 de diciembre de 1992, p.3. Por otra parte, aunque el Convenio hace referencia a la obtención de la información sin gastos excesivos", no obstante la Ley silencia esta cuestión. Si bien dice que el Registro es gratuito (art. 13) y que no se exigirá contraprestación alguna por la rectificación o cancelación de los datos de carácter personal inexactos (art. 16.2), en la regulación reglamentaria del procedimiento para el ejercicio del derecho de acceso se podría establecer el pago de un canon.

■ 59 Se refiere al artículo 20. Ficheros de las Fuerzas y Cuerpos de Seguridad.

chos 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".

Artículo 22. Otras excepciones a los derechos de los afectados.

" 2. Lo dispuesto en el artículo 14 y en el apartado 1 del 15[60] 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..."

Sobran los comentarios. El último de estos preceptos (art.22) ha conducido, -como en su momento adelantamos-, a plantear sendos recursos de inconstitucionalidad al Defensor del Pueblo y al Grupo Parlamentario Popular[61], sosteniendo que las excepciones que en el mismo se establecen pueden rebasar las dispuestas en el Convenio 108[62].

Por lo tanto, el Sr. Olaverri cuando ejercite el derecho de acceso (o el de rectificación y cancelación) podrá encontrarse con estas limitaciones. Aun así, hay que recordar, (y en esto no nos detenemos pues excede el objeto de estudio), que también corresponde a la Agencia de Protección de Datos, como órgano de tutela el resolver, a instancia del interesado, la procedencia o improcedencia de la denegación de estos derechos[63].

Por último recordar que nos hemos centrado en los derechos de información y de acceso, pues tales eran los derechos tratados en esta sentencia. Sin embargo, y, como en su momento mencionamos, la LORTAD establece otra

- 60 Se refiere al artículo 14. Derecho de acceso y al artículo 15. Derecho de rectificación y cancelación.
- 61 Además también se recurren otros preceptos. Sobre el Boletín Oficial del Estado que recogía estos extremos dábamos cuenta en nota 9.
- 62 En la nota 9 citábamos los autores que se han ocupado de los puntos más críticos de la ley. A ella nos remitimos.Si bien sobre este particular, pues lo tratan más detenidamente, cabe destacar a D. LOPEZ GARRIDO, "El Proyecto de Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal...", cit., pp. 17 y ss., M. HEREDERO HIGUERAS, "La ley orgánica 5/1992, de 29 de octubre,...", cit., pp. 2101-2104, así como la obra citada de P. LUCAS MURILLO DE LA CUEVA, "Informática y Protección de datos personales...", cit., 101-111.
- 63 El artículo 21.3 y 22.2 de la Ley establece la posibilidad de poner en conocimiento del Director de la Agencia la negativa del derecho de acceso. Asimismo el art. 12.2 del EAPD dispone que corresponde al Director de la Agencia: " Resolver motivadamente sobre la procedencia o improcedencia de la denegación, total o parcial, del acceso a los ficheros policiales o tributarios automatizados" .

serie de derechos: Derecho de rectificación y cancelación (art. 15), derecho de indemnización (art. 17), derecho a la reclamación ante la Agencia (art.17).También ellos forman parte de la vertiente positiva, activa del derecho a la autodeterminación informativa .En consecuencia, el demandante, si es el caso, los podrá ejercitar.

IV. El derecho a la intimidad y el derecho a la Autodeterminación Informativa. Otras Denominaciones: El derecho a la libertad informática y el derecho a la privacidad. La posición del Tribunal Constitucional.

La estrecha conexión del derecho a la intimidad con la protección de los datos personales no se puede poner en tela de juicio. De hecho, la protección ante la informática arranca de este derecho. Sin embargo, en mi opinión, como muy acertadamente señala JIMENEZ ESCOBAR, esta innegable relación ha eclipsado el verdadero problema. Al ligar el derecho a la intimidad con la protección de los datos personales se ha producido una sustitución, "...por un concepto relacionado, pero distinto, cual es el ataque a la intimidad"[64] .

La concepción del binomio informática-intimidad como un hecho indisoluble ha originado que, en el Estado, numerosos estudios, conferencias, trabajos, opiniones etc (salvando notorias excepciones a las que nos referiremos en párrafos posteriores) hayan sido "víctimas" de estas circunstancias . Dicho error , que se ha ido extendiendo y consolidando con el paso del tiempo, también encuentra, a mi modo de entender, sus manifestaciones en esta sentencia del Tribunal Constitucional que estamos analizando .

En cualquier caso, y antes de proceder a la "detección" de tales manifestaciones en el recurso de amparo que nos ocupa, interesa saber cuáles son las razones que han originado que el binomio informática-derecho a la intimidad se muestre a nuestro ojos como una verdad indiscutible para posteriormente destacar el papel magistral desempeñado por cierto sector de la doctrina que ante esta confusión reinante ha sabido enfocar (y enfoca) adecuadamente el problema de la protección de los datos personales.

JIMENEZ ESCOBAR señala que el derecho ante el problema, y necesidad, que suponía encuadrar este fenómeno nuevo de la irrupción informática

■ 64 Se sigue a R. J JIMENEZ ESCOBAR, ' Informática y derecho a la intimidad:una concepción que debe arrumbarse" en Jornadas Abogacía e Informática..., cit., p.85 .

en una categoría jurídica, encontró en la intimidad la respuesta jurídica adecuada. "El derecho a la intimidad era una libertad fundamental perfectamente estudiada, nacida como categoría jurídica el siglo pasado y sin el abolengo de otros derechos humanos, pero totalmente definida, acotada, documentada. Acudir a esta categoría evitaba la fatigosa tarea de crear un nuevo derecho (o el tener que prescindir de un determinado derecho) al que designar como objeto de la agresión de la nueva tecnología"[65] .

Este autor añade además, que en numerosas ocasiones la agresión a la intimidad, es un antecedente previo y necesario para la posterior recogida, tratamiento y comunicación ilegítimos de los datos de carácter personal (se realizan estos procesos sin su consentimiento, por ejemplo, cuando éste debe ser requerido). Esto ha generado una confusión entre el fenómeno y su premisa.

Las causas ahí están. Sin embargo, esto no ha impedido que desde hace ya años, desde casi recién aprobada la Constitución, el profesor PEREZ-LUÑO, cuyos estudios en materia de protección de datos han alcanzado el máximo reconocimiento[66], se mostrará crítico ante el dogma establecido por el binomio intimidad-informática.

Posteriormente, y sobre todo a partir de 1984, este autor comienza a utilizar en sus escritos la expresión "derecho a la autodeterminación informativa"[67], (cabe destacar la excelente defensa que de su uso mantiene en los últimos años el constitucionalista LUCAS MURILLO DE LA CUEVA[68]) denominación que desplaza en lo que se refiere a la cuestión de los datos personales al derecho a la intimidad. La sentencia del Tribunal Constitucional Federal alemán sobre la Ley del Censo de Población de 15 de diciembre de 1983 constituye un hito fundamental en la afirmación del derecho a la autodeterminación informativa. Este nuevo derecho de construcción jurisprudencial (en la Ley Fundamental de Bonn no se encontraba ninguna referencia literal a este precepto) se refiere al derecho de toda persona a controlar el flujo de

- 65 R. JIMENEZ ESCOBAR, "Informática y derecho a la intimidad...", cit., p.85.
- 66 La enumeración de sus obras sobre esta materia sería muy prolija. Citaremos entre otros algunos de sus más antiguos escritos. A. E. PEREZ-LUÑO, La protección de la intimidad frente a la informática en la Constitución de 197' en Revista de Estudios Políticos, n° 9. Madrid, 1979; Informática y libertad. Comentario al art. 18.4 de laC.E." también en Revista de Estudios Políticos, n° 24. Madrid, 1981; "La defensa del ciudadano y la protección de datos" en Jornadas Internacionales sobre Informática y Administración Pública", cit., pp. 55 y ss; " La contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo", en Anuario d e Derechos humanos, n°4, 1986-1987.
- 67 Así, A. E. PEREZ-LUÑO en " La defensa del ciudadano y la protección de datos. . . ", cit., pp.55 ss; "Libertad informática y Derecho a la autodeterminación informática". Congreso sobre Derecho Informático, cit. ,pp. 359 y ss; o en Los derechos humanos en la sociedad tecnológica. . .", cit., pp. 155 y ss.
- 68 P. LUCAS MURILLO DE LA CUEVA, "El derecho a la autodeterminación informaUva", Ed. tecnos, Temas clave, Madrid, 1990; P. LUCAS MURILLO DE LA CUEVA, "La protección de los datos personales ante el uso de la informática " (I parte) y (II parte), cit.,; " Informática y Protección de datos personales...", cit.

informaciones que a él le conciernen -tanto en la recolección como el posterior tratamiento y uso de los datos personales- mediante toda una serie de derechos subjetivos como el consentimiento, el derecho de acceso, rectificación, etc.

Centrándonos en el recurso de amparo, objeto de nuestro estudio, se observa la presencia de ambas corrientes. Veámoslo:

"...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"."

Y añade en el siguiente fundamento jurídico:

"La llamada "libertad informática" es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)."

Como vemos el Constitucional se refiere a un nuevo derecho, que califica de derecho de libertad, (libertad informática), el cuál es además garantía de otros derechos, especialmente el honor y la intimidad. Sin perjuicio de que posteriormente nos detengamos en la doble naturaleza de este "instituto" como derecho y garantía, lo importante en estos momentos es destacar que de las anteriores palabras del TC se deduce una filosofía y una concepción del 18.4 muy semejante a la mantenida por la doctrina anteriormente expuesta. Quizás en el Constitucional se observa una mayor reticencia a dar un nombre a este nuevo derecho, -tímidamente se refiere a él como libertad informática frente a la expresión "derecho a la autodeterminación informativa" denominación más frecuentemente utilizada[69].

Sin embargo, curiosamente a lo largo del resto de los fundamentos jurídicos de esta sentencia el Constitucional abandona este lenguaje que incipientemente había empleado, y para referirse a la misma realidad que hemos comentado se decanta por la expresión "derecho a la intimidad":

■ 69 Así P. LUCAS MURILLO DE LA CUEVA dice: "El bien jurídico subyacente es la libertad informática o -en fórmula menos estética pero más precisa- la autodeterminación informativa". P.LUCAS MURILLO DE LA CUEVA "La protección de los datos personales ante el uso de la informática..." (I parte), cit., p. 17.

"...impide aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas.." (f. jco 7)

"...dichas facultades de información forman parte del derecho a la intimidad.." (f. jco 7)

"... la Administración demandada en este proceso vulneró el contenido esencial del derecho a la intimidad del actor..." (f. jco 8)

"...Pero ello no desvirtúa el fundamento constitucional de tales derechos[70], en cuanto imprescindibles para proteger el derecho fundamental a la intimidad en relación con los ficheros automatizados que dependen de los poderes públicos." (f. jco 9), etc.

En estas citas el TC habla del derecho a la intimidad, unas veces como derecho que posee además una vertiente positiva, (derecho a controlar las informaciones, por medio de los derechos de información y acceso) y otras como el derecho que queda protegido por medio de estos derechos instrumentales.

Quizás el cambio en la terminología empleada obedece a que a lo largo de estos fundamentos jurídicos, el Constitucional se ocupa de responder al Ministerio Fiscal y al Abogado del Estado, los cuáles hablan continuamente del derecho a la intimidad.

La utilización de las expresiones derecho a la intimidad y derecho a la autodeterminación informativa como sinónimas nos confirman que el "error" también ha sido obviado por el Constitucional.

Además de las razones anteriormente apuntadas cabría añadir algunas otras para "arrumbar definitivamente el binomio derecho a la intimidad-informática".

Mantener que el derecho a la intimidad es el marco adecuado para la protección de los datos personales significaría afirmar que este derecho ha ampliado su campo de protección de una manera extraordinaria. LUCAS MURILLO DE LA CUEVA señala que esta interpretación le convertiría, en la práctica, en un derecho general de la personalidad y sería sumamente difícil la organización de una tutela jurídica que resultara eficaz para un bien de contornos imprecisos y de una naturaleza totalmente dinámica. Además habría que

■ 70 Se refiere al derecho de información y de acceso.

modificar la catalogación de ciertos datos que en el normal entendimiento, en el entendimiento cotidiano no se reconocen como íntimos[71] .

Hechos que no guardan ninguna relación con la intimidad como el supuesto de tener o no un automóvil o de ser cliente de una entidad financiera determinada, (ejemplos señala LUCAS MURILLO DE LA CUEVA[72]) u otros hechos (puestos de relieve por JIMENEZ ESCOBAR[73]) como la raza, la adicción religiosa o la filiación política o la conducta sexual cuando se explicita públicamente en determinados colectivos como forma de protesta, no pueden ser considerados íntimos. Sin embargo, todos estos hechos, y -especialmente estos últimos que aunque han perdido la condición de íntimos por hacerlos públicos la persona- necesitan una tutela legal frente a su tratamiento automatizado, cesión, etc.

La técnica de la protección de datos no se centra ni mucho menos con exclusividad en lo que se viene entendiendo como intimidad. En opinión de LUCAS MURILLO DE LA CUEVA, "si este fuese el bien jurídico por defender, la que habría que resguardar del peligro informático sería bastante poco". Sin embargo ciertos datos que en principio parecen inocuos, o datos que pueden ser sensibles pero no íntimos son los que entran de lleno en el bien jurídico nuevo que se protege: la libertad informática y que da lugar al nacimiento de un nuevo derecho fundamental, el derecho a la autodeterminación informativa.

Por su parte, la LORTAD tampoco menciona este derecho a la autodeterminación informativa, sin embargo resulta sumamente interesante su distinción entre la intimidad y la privacidad.

"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: aquella 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 las 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 persona-

- 71 p LUCAS MURILLO DE LA CUEVA, " La protección de los datos personales ante el uso de la informática ..." I parte), cit., pp. 15-18.
- 72 P.LUCAS MURILLO DE LA CUEVA, "La protección de los datos personales ante el uso de la informática..." (I parte), cit., p. 16.
- 73 R. JIMENEZ ESCOBAR, "Informática y derecho a la intimidad:una concepción que debe arrumbarse" en Jornadas Abogacía e Informática..., cit., p.85 .

lidad 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."

De estas reflexiones del TC se concluye fácilmente que lo que el legislador llama privacidad viene a coincidir prácticamente con lo que se ha venido denominando por la doctrina autodeterminación informativa[74] . De esta manera, esta coincidencia se puede comprobar si se compara el texto que hemos subrayado del concepto de privacidad recogida en la Exposición de Motivos de la LORTAD con la formulación del derecho a la autodeterminación informativa en su nacimiento, en la famosa Sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983

El Tribunal Federal Constitucional señala:

"De este modo un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, ya no existe, bajo la elaboración automática de datos, ninguno "sin interés".

A pesar de que hubiese sido preferible el empleo por parte del legislador de la expresión derecho a la autodeterminación informativa -pues como hemos tenido ocasión de comprobar, ésta ya ha sido utilizada y estudiada por doctrina de peso- la preferencia por el término privacidad, como bien jurídico diferente del de la intimidad, permite, al igual que esta otra expresión, referirse a un nuevo derecho cuyo ámbito supera el que es comúnmente objeto de protección del derecho ala intimidad. Así en la Exposición de Motivos de la Ley se indica que mediante el desarrollo legislativo del 18.4 de la Constitución se obtiene "una protección reforzada de los derechos fundamentales del ciudadano, En este caso, al desarrollar legislativamente el mandato constitucional de limitar el uso de la informática, se está estableciendo un nuevo y más consistente derecho a la privacidad de las personas".

■ 74 Así lo afirma LUCAS MURILLO DE LA CUEVA quién además añade que también se llega a esta misma conclusión al comprobar que la LORTAD establece como principio básico inspirador y como uno de los derechos de las personas el de consentimiento o el de autodeterminación "que otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes" . P. LUCAS MURILLO DE LA CUEVA, "La protección de los datos personales ante el uso de la informática .. ." (1 parte), cit., p. 18.

Hasta ahora nos hemos decantado por la preferencia de la expresión derecho a la autodeterminación informativa (y en menor medida, pero también aceptable de esta otra, recogida en la LORTAD, derecho a la privacidad) como marco adecuada para la protección de datos personales. En mi opinión, sería sumamente importante por las razones indicadas, que se produzca el necesario deslinde entre el derecho a la intimidad y el derecho a la autodeterminación informativa.

Las referencias al derecho a la intimidad frente al uso de la informática y al derecho a la libertad informática empleadas por el TC en este recurso de amparo para referirse a realidades idénticas obedece a las causas que hemos ido apuntando. Ante los peligros del fenómeno informático se encontraba una respuesta inicial en un derecho que era perfectamente conocido y estudiado, el derecho a la intimidad. Además, y ya lo señalábamos como otra posible disculpa, es cierto que es el derecho a la intimidad el que queda vulnerado en muchos casos, cuando de manera ilegítima se recogen, tratan y comunican datos.

Sin embargo, a pesar de que estas razones conducen a la doctrina y hasta al propio Tribunal Constitucional a seguir siendo "víctimas" de la expresión derecho a la intimidad, hay que hacer una apuesta fuerte por la utilización de otra terminología perfectamente acuñada como es la del derecho a la autodeterminación informativa.

La figura del responsable del fichero de datos de carácter personal en la LORTAD

EMILIO DEL PESO NAVARRO

Licenciado en Derecho y en Informática.
Miembro de la Asociación de licenciados en Informática.

SUMARIO

INTRODUCCION

DEFINICION DE LA FIGURA EN DIFERENTES ORDENAMIENTOS JURIDICOS

EL RESPONSABLE DEL FICHERO EN LA LORTAD

PERFIL DEL RESPONSABLE SEGUN LA LEY

RESPONSABILIDADES

CONCLUSIONES

LEGISLACION Y DOCUMENTACION

BIBLIOGRAFIA CONSULTADA

Introducción

La falta de una ley de protección de datos que desarrollase el artículo 18.4 de la Constitución de 1978 ha sido, durante muchos años, una de las asignaturas pendientes de nuestro ordenamiento jurídico.

Esta laguna legal, pendiente de regulación durante tantos años, ha desaparecido recientemente con la promulgación de la Ley Orgánica 5/1992 de 26 de octubre, publicada en el Boletín Oficial del Estado número 262 de 31 de octubre de **Regulación del Tratamiento Automatizado de los Datos de carácter personal**, la ya célebre **LORTAD**.

Esta Ley con sus virtudes y defectos, ha supuesto indudablemente un paso adelante en el camino hacía la defensa de la intimidad de la persona, entendida ésta en un sentido amplio.

No vamos a entrar aquí, pues pensamos que no es el objeto de este estudio, a analizar qué se entiende por intimidad y por privacidad y qué parte de nuestro entorno informativo corresponde a cada una de ellas.

La Ley promulgada, uno de cuyos vicios estimamos que es la contínua remisión a la vía reglamentaria para el desarrollo de su articulado, debe dar origen a un Estatuto y dos Reglamentos.

El Estatuto de la Agencia de Protección de Datos ya ha sido aprobado por el Real Decreto 428/1993 de 26 de marzo y publicado en el Boletín Oficial del Estado número 106 de 4 de mayo.

Los Reglamentos, que según el artículo 5 del Estatuto han de ser informados por la Agencia de Protección de Datos se referirán:

a) uno a los aspectos puramente técnicos relacionados con la seguridad de la información y a la forma en que ésta ha de ser aplicada por los responsables de los ficheros.

b) el otro deberá ser de propósito general para desarrollar los numerosos artículos pendientes de ello.

La publicación de la Ley ha creado, como hemos observado, cierta alarma en los medios empresariales y ha servido también para llevar la inquietud a más de un directivo del sector privado.

Esto no ha sido así, o por lo menos no hemos sido capaces de detectarlo, en el sector público.

Esta situación, fácil de adivinar en las numerosas reuniones en las que hemos participado a partir de la publicación de la Ley, tiene dos facetas claramente diferenciadas: una empresarial y otra personal.

Respecto de la primera hemos de decir que está principalmente motivada por la inexistencia en el mundo empresarial español de una cultura de la seguridad en sus tres aspectos físico, lógico y jurídico.

En otros países, además de dar mayor importancia a los problemas relacionados con la seguridad, han pasado ya por tres generaciones de leyes de protección de datos y por tanto la entrada en vigor de leyes de este tipo no ha supuesto ningún trauma pues esa cultura de la seguridad se ha ido imponiendo poco a poco y su aplicación no ha representado grandes sacrificios económicos.

Hemos de tener en cuenta que en algunos países europeos las primeras leyes de protección de datos son de los años setenta.

En aquella época la informática estaba recluida, por decirlo así, en grandes centros; se trataba de una informática totalmente centralizada.

Implantar un sistema de seguridad en esas circunstancias era relativamente fácil y su coste no muy elevado, aunque la tecnología en esta materia no estuviese muy avanzada.

Posteriormente, al pasarse a una informática distribuida en esos países, ya existía una cultura empresarial de la seguridad y no se partía de cero, por lo que el salto a esos sistemas de seguridad más sofisticados no fue tan traumatizante ni costoso.

En la actualidad, con la incorporación de los ordenadores personales a las empresas y a las Administraciones Públicas, se ha agudizado el problema; pero, como en el caso anterior, aquellos países cuyos empresarios y gestores públicos fueron conscientes de la necesidad de proteger la información con adecuadas medidas de seguridad han podido pasar de unos sistemas a otros sin demasiadas dificultades.

En nuestro país la aplicación de la ley sí va a traer consigo considerables desembolsos económicos al tenerse que implantar esos sistemas de seguridad que ya debían funcionar y que, salvo en casos excepcionales, no existen.

En estos últimos años se ha avanzado bastante en el área de la seguridad física de los equipos informáticos pero aún queda mucho por hacer en el campo de la seguridad lógica de la información tanto en las propias instalaciones como en la transmisión de la información a través de líneas telefónicas. La seguridad jurídica, tercer aspecto a contemplar, viene a ser garantizada por esta nueva ley.

La Criptografía, imprescindible en muchos casos, principalmente en la transmisión de información a través de las redes telemáticas, aún es una desconocida en la mayoría de las instalaciones informáticas.

Es importante resaltar que hasta el momento presente en muchas empresas los datos de carácter personal han sido datos de segunda categoría toda vez que la preocupación principal estaba en garantizar la seguridad y la integridad de los datos de carácter simplemente económico que eran los que se tenían que cuadrar y que podían reflejar el estado financiero de la empresa, teniendo más importancia que los datos de carácter puramente personal.

La importancia que la aplicación de esta ley tiene para las empresas nos ha llevado en alguna ocasión a tener que advertir, en las reuniones en que hemos participado, que el objeto de la misma no es regular el sistema de seguridad de los ficheros de las empresas con todas las implicaciones que esto conlleva, sino desarrollar un derecho fundamental de la persona que figura en el Título I de nuestra Constitución.

Respecto a la inquietud personal creada en nuestros ejecutivos hay que pensar que aunque la ley en su artículo 3° al definir al responsable del fichero dice que éste puede ser una persona jurídica de naturaleza pública o privada, prácticamente nadie tiene en cuenta esa posibilidad y ve a la figura del responsable del fichero con nombre y apellidos propios.

Estas personas son conscientes de las dificultades y responsabilidades del cargo.

Debido a esta inquietud, a ese interés por esta figura reflejado en las múltiples preguntas que nos han efectuado es por lo que hemos elegido este tema para tratar con ello de llamar un poco la atención de los estudiosos sobre el mismo y así poder entre todos cerrar esas interrogantes que aún permanecen abiertas sobre una figura que empieza a ser controvertida.

Definición de la figura en diferentes ordenamientos jurídicos.

Vamos a examinar a continuación cómo se define esta figura en diferentes ordenamientos jurídicos de nuestro entorno cultural y económico, teniendo en cuenta que no en todos recibe el nombre de responsable del fichero sino que varía; variación que en algunos casos afecta al contenido propio de sus funciones.

Hemos advertido que según las leyes van siendo más modernas la figura es tratada con más minuciosidad y al mismo tiempo adquiere mayor importancia.

Ley Alemana federal de Protección de Datos de 27 de enero de 1977.[1]

Art. 2

A los efectos de la presente ley se entenderá por:

1.- "ente almacenante" cualquiera de las personas o entes mencionados en el artículo 1, segundo párrafo, proposición primera, que almacenare datos por sí mismo o encomendare a otros su almacenamiento.

En el artículo 39 referido al deber de dar cuenta de la iniciación de la actividad en sus puntos 1 y 2 figuran:

1.- nombre o denominación del ente.

2.- propietario, directiva, gerente u otro director designado en virtud de disposición legal o estatutaria, y personas encargadas de la dirección del tratamiento de datos.

Ley de Protección de Datos Personales de Austria de 18 de octubre de 1978.[2]

Art. 2.3

A los efectos de las disposiciones que siguen de la presente Ley federal se entenderá:

- 1 Julio Téllez Valdés. Derecho Informático. Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas. México 1987. Pág. 143.
- 2 Informática. Leyes de Protección de Datos (III). Documentación Informática Nº 2. Presidencia del Gobierno. Secretaría General Técnica. Madrid 1977. Pág. 27.

3. Por **"comitente"** todo ente de Derecho Público o todo órgano de una corporación territorial, por el cual fueren elaborados datos, bien directamente, bien con intervención de prestadores de servicios, con ayuda de medios automatizados.

Convenio del Consejo de Europa para la protección de las personas con relación al tratamiento automatizado de datos de carácter personal de 28 de enero de 1981.[3]

*Art. 2 Definiciones.

A los efectos del presente Convenio las expresiones que se relacionan tendrán los significados o contenidos que respectivamente se detallan:

d. **"responsable de los datos"** significará la persona física o jurídica, autoridad pública, servicio u otro organismo que según la ley nacional fuere competente para decidir sobre que clases de datos de carácter personal deben ser almacenadas y qué operaciones deberán serles aplicadas.

Ley de Datos de Datos de Suecia de 3 de junio de 1982.[4]

Art. 1. En la presente ley se entenderá:

- por "**responsable del registro**", la persona mediante cuya actividad se llevare el archivo de personas, si la misma dispusiere del registro.

Ley de Protección de Datos del Reino Unido de 12 de julio de 1984.[5]

1.-

Por **"usuario de datos"** se entenderá la persona que retiene datos en su poder, entendiéndose que una persona "retiene" en su poder datos si se dan las condiciones siguientes:

a) que los datos formen parte de un conjunto de datos procesados o que hubieren de serlo por o por cuenta de una persona, según se indica en el párrafo segundo; y

- 3 Julio Téllez Valdés. Obra cit. pág. 210.
- 4 Informática. Leyes de Protección de Datos (III). Obra cit. Pág. 367.
- 5 Id. id. Pág. 305.

b) que dicha persona (separadamente o mancomunada o solidariamente con otras personas) decide sobre el contenido y uso de los datos incluido en el conjunto de datos; y

c) que los datos revistieren la forma en la cual hubieren sido procesados o debieren serlo, según se indica en el apartado a) o (aun cuando a la sazón no revistieren tal forma) una forma a la cual hubieren sido reconvertidos después de haber sido procesados y con miras a seguir siéndolo con posterioridad.

Un Proyecto de ley italiana de Protección de Datos de Mario G. Losano.[6]

(Se trata de un proyecto puramente técnico por lo que es interesante compararlo con los demás que suelen el resultado de un pacto político).

Art. 14. Nombramiento del responsable para la protección de los datos personales.

1) Los sujetos obligados deben nombrar, previo dictamen de las organizaciones sindicales internas, al responsable para la protección de los datos personales.

2) A él han de dirigirse los interesados a fin de ejercitar los derechos informáticos reconocidos en el presente Título segundo, y los garantes públicos en el desarrollo de sus funciones de inspección y de control.

3) El responsable de los bancos de datos personales:

a) Debe estar en posesión de una acreditada experiencia organizativa, informática y jurídica.

b) Debe estar sujeto a la dependencia directa de la cúpula de la dirección empresarial, o bien en las administraciones públicas y en los entes de derecho público, los respectivos órganos ejecutivos.

c) En función de las dimensiones de los bancos de datos personales, el cargo de responsable puede compatibilizarse con otras tareas de gestión o de dirección, siempre que ello no perjudique el cumplimiento de las tareas que le, han sido atribuidas en el ámbito de la protección de los datos personales.

■ 6 Mario G. Losano, Antonio Enrique Pérez Luño y María Fernanda Guerrero Mateus. Libertad Informática y Leyes de Protección de Datos Personales. Cuadernos y Debates Nº 21. Centro de Estudios Constitucionales. Madrid 1989. Pág. 175.

Art. 15. Funciones del responsable para la protección de los datos personales.

1) Al responsable de los datos personales se le atribuyen las siguientes funciones:

a) La elaboración de la normativa interna necesaria para garantizar el puntual cumplimiento de la presente ley, así como el control formal sobre su aplicación.

b) La creación, la gestión y la actualización del registro de los bancos de datos personales puestos en funcionamiento por parte del sujeto obligado.

c) La comunicación de las informaciones necesarias, respectivamente, para los interesados a fin de ejercitar sus derechos informáticos y para los garantes públicos a fin de ejercitar sus funciones.

d) Recibir las reclamaciones de los interesados que estimen lesionado un derecho constitucionalmente garantizado a causa de la memorización de datos personales; incluirlas en el orden del día de la Comisión, a fin de constituir, cuando sea necesario, el grupo de trabajo que examine la queja;

e) Las observaciones y las sugerencias, dirigidas bien a la dirección empresarial, bien a los garantes públicos, a fin de modificar la presente ley y de adecuar su aplicación.

Art. 16. Responsabilidad.

1) De las funciones a que se refiere el precedente art. 15 responde por sí mismo el responsable de los datos personales; no le son sin embargo imputable las violaciones materiales a la normativa interna, que no se pueden detectar a través del control formal de su competencia.

Distingue claramente este Proyecto entre titular del fichero, al que denomina "sujeto obligado", y el "responsable del fichero".

Al primero dedica los artículos 3, 5, 11 y 12 y el segundo los artículos 14 y 15.

Propuesta de Directiva de la Comunidad Económica Europea de 18 de julio de 1990

En el texto de la propuesta anterior a la modificación de 15 de octubre de 1992 en su artículo 2 e) figuraba "responsable del fichero", la persona natural o jurídica, autoridad pública, servicio o cualquier otro organismo que, con arreglo al Derecho Comunitario o a la legislación de un Estado miembro, sea competente para decidir la finalidad del fichero, qué categorías de datos personales deben registrarse, qué operaciones deben aplicárseles a éstos y a qué terceros está permitido el acceso a los mismos;"

En el texto modificado desaparece esta figura y aparecen tres nuevas: responsable del tratamiento, encargado del tratamiento y tercero (art. 2 d,e y f).

"d) "responsable del tratamiento", la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate u ordene tratar datos personales y decida acerca de la finalidad y los objetivos del tratamiento, los datos personales que deben tratarse, las operaciones que deben aplicárseles y los terceros que pueden tener acceso a dichos datos;

"e) "encargado del tratamiento", la persona física o jurídica que trate datos personales por cuenta del responsable del tratamiento;"

"f) "terceros" las personas físicas o jurídicas con excepción del interesado, del responsable del tratamiento y de las personas autorizadas para tratar los datos bajo su autoridad directa o por su cuenta;

En los Comentarios a la modificación del Proyecto de Directiva, como veremos más adelante se justifica este cambio de terminología.

Del examen de las leyes precedentes, se desprende que prácticamente todas, salvo el proyecto italiano de LOSANO, contemplan la posibilidad de que el responsable del fichero sea un colectivo; así vemos que en la ley alemana puede ser una directiva; en la austríaca, se entiende por comitente, un ente de derecho público o un órgano de corporación territorial; el convenio del consejo de Europa, reflejado en nuestra ley de protección de datos, admite como responsable de los datos personas físicas, jurídicas, autoridades públicas, servicios u otros organismos y el usuario de datos del Reino Unido es el quien solo o mancomunada o solidariamente con otras personas decide sobre el contenido.

El proyecto de directiva de la Comunidad, en su última versión, sigue esta línea de posibilitar que el responsable del tratamiento pueda ser persona física, jurídica, autoridad pública, servicio u organismo.

El Proyecto italiano de LOSANO al establecer las condiciones que debe reunir el responsable para la protección de los datos personales se refiere a una persona física.

Esto es así porque anteriormente ha establecido otra categoría, la de sujetos obligados en realidad titulares de los ficheros, quienes sí podrán ser personas colectivas.

El responsable del fichero en la LORTAD.

Responsable, según la vigésima primera edición correspondiente al año 1992 del Diccionario de la Lengua Española de la Real Academia en sus diferentes acepciones es:

- El obligado a responder de alguna cosa o por alguna persona.

- Dícese de la persona que pone cuidado y atención en lo que hace o decide.

- También se dice de la persona que tiene a su cargo la dirección y vigilancia del trabajo en fábricas, establecimientos, oficinas ni muebles, etc.

A los efectos de la LORTAD, según su artículo 3 d) "responsable del fichero" es: "persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento".

La definición, como se recordará, es similar a la que figura en el Convenio del Consejo de Europa.

La figura del responsable del fichero aún no siendo el objeto de la ley, pues éste es la protección de los datos de carácter personal, indudablemente es uno de los ejes sobre los que el legislador hace girar la misma.

Esta figura aparece veinticuatro veces en la ley en diecinueve artículos; su actuación, por consiguiente, es muy importante para la correcta aplicación de la misma.

Asimismo en el Estatuto de la Agencia de Protección de Datos también aparece ocho veces en cuatro artículos.

A continuación vamos a analizar esta interesante figura, partiendo de su definición en la propia ley.

La LORTAD se refiere muchas veces al responsable del fichero pero no dice nada, o mejor dicho, dice muy poco del titular del mismo.

Para LOPEZ-MUÑIZ GOÑI y RODRIGUEZ ARRIBAS [7] "dado el tratamiento que se hace de esta figura, no parece muy acertado el nombre de "responsable" del fichero, sino que corresponde más al concepto de "titular" o propietario puesto que es el que define cuál va a ser la finalidad del mismo, datos que va a contener y forma de uso del tratamiento."

En los Comentarios a 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 a la libre circulación de estos datos al analizar la figura del "responsable del tratamiento" se dice que: "se trata de la persona responsable, en última instancia, de las opciones escogidas a la hora de determinar y llevar a cabo los tratamientos, (en la mayoría de los casos, el jefe de empresa), y no de las personas que efectúan las operaciones de tratamiento de acuerdo con las instrucciones del responsable, razón por la cual se indica que es el responsable quien decide "los objetivos" del tratamiento.

El responsable del tratamiento puede tratar los datos por sí mismo o hacer que los traten los miembros del personal a su cargo o al agente tratante, persona jurídicamente diferente del responsable pero que actúa por cuenta de él".

A nuestro juicio la definición de "responsable del fichero" que aparece en el art 3 d) de la ley no se corresponde con el uso que de dicha figura se hace a través de la misma.

Entendemos que en la práctica existen dos figuras claramente diferenciadas: el titular del fichero y el administrador de los datos.

Dichas figuras pueden coincidir en algunos casos en una misma persona debido, por ejemplo, a la dimensión de la empresa.

El titular del fichero puede ser una persona física, jurídica de naturaleza pública o privada o un organismo público; el administrador de los datos necesariamente ha de ser una persona física.

■ 7 Miguel López-Muñiz Goñi y Ramón Rodriguez Arribas. Infracciones y sanciones en la Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. 5º Congreso Internazionale sul tema: Informática e attività giurídica. Corte Suprema di Casazione. Roma mayo 1993, Pág. 5.

En la ley se introduce una nueva figura la del responsable del fichero que unas veces aparece claramente diferenciado del titular del mismo y otras no tanto.

Con la creación de esta figura, se ha querido buscar en cierto modo un "chivo expiatorio" sobre el que recaiga la responsabilidad del cumplimiento de la ley. Se quiere que siempre exista un responsable de los daños que se puedan ocasionar.

Esta responsabilidad queda, en cierto modo, diluida con la posibilidad de que el responsable pueda ser una persona jurídica pública o privada e inclusive un organismo público.

A continuación vamos a examinar cómo es contemplada esta figura en la ley y de dicho examen tratar de obtener un perfil del responsable del fichero y asimismo deducir cuáles son sus responsabilidades.

Respecto a la identidad del responsable del fichero existe, según la ley:

Deber de publicidad

- De la identidad y dirección del responsable del fichero deberá ser informado el afectado al que se soliciten datos personales (art 5).

- El Registro General de Protección de Datos informará a quien se lo solicite de la identidad del responsable del fichero (art 13).

- Las disposiciones de creación o de modificación de ficheros de titularidad pública deberán indicar los órganos de la Administración responsables del fichero automatizado (art 18).

- Toda persona o entidad que proceda a la creación de ficheros automatizados de datos de carácter personal deberá notificar a la Agencia de Protección de Datos el nombre del responsable del fichero (art 24.1 y 2).

- Asimismo deberá comunicarse a la Agencia de Protección de Datos cuando se cambie el responsable del fichero (art 24.3).

- En los asientos de inscripción de los ficheros de titularidad pública figurarán los órganos de la Administración responsables del fichero automatizado (art 24.2 del Estatuto).

- En los asientos de inscripción de los ficheros de titularidad privada figurará el nombre del responsable del fichero así como los cambios del mismo que se hayan efectuado (art 24.3 del Estatuto).

De lo anterior se desprende el interés del legislador en que la identidad del responsable del fichero sea suficientemente conocida y así saber a quien exigir responsabilidad por las actuaciones ilícitas que se produzcan no ocurra como antes de la promulgación de la ley en que muchas veces era difícil conocer quien era el responsable por no estar claramente establecida la identidad del mismo.

El responsable del fichero en el desempeño de sus funciones tiene una serie de deberes:

Deber de seguridad de los datos

"El responsable del fichero deberá adoptar las medidas de índole técnica y organizativa 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." (art 9.1)

Este deber de seguridad de los datos es muy importante y de su adecuada adopción depende en gran modo la protección que se pretende con la ley.

La labor del responsable del fichero en este caso es puramente técnica y le separa, en este caso, de aquel acercamiento que vimos anteriormente que tenía la figura respecto a la del titular del fichero.

Deber de secreto

"El responsable del fichero automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo" (art 10).

En este artículo se hace una clara distinción entre el titular del fichero y el responsable del mismo.

En el Proyecto de Ley Orgánica de Código Penal publicado en el Boletín Oficial de las Cortes Generales-Congreso de Diputados número 102-1 de 23 de

setiembre de 1992 en el Capítulo I del Título IX referido a los delitos contra la intimidad y el secreto de las comunicaciones en su artículo 198 al referirse a quienes "se apoderasen de datos reservados de carácter personal o familiar de otro, registrados en ficheros de archivo o registro, público o privado" (art 198.2) y "a quienes difundieren o revelaren a terceros los datos reservados descubiertos" (art 198.3) agrava las penas "si los hechos se realizaren por las personas encargadas o responsables de los ficheros, soportes informáticos, archivos o registros" (art 198.4).

Este Proyecto de ley, como es sabido, no ha podido seguir su curso parlamentario debido a la anticipada disolución de las Cámaras, aunque es de esperar un nuevo proyecto para la próxima legislatura.

Deber de rectificación y cancelación de datos personales

- El responsable del fichero "tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del afectado" (art 15).

Deber de indemnización

"3. Los afectados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable del fichero sufran daño o lesión en sus bienes tendrán derecho a ser indemnizados.

4. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

5. En el caso de los ficheros de titularidad privada la acción se ejercitará ante los órganos de la jurisdicción ordinaria." (art 17)

Deber de información al afectado

- El responsable del fichero deberá facilitar el derecho de acceso del afectado del artículo 14 (a contrario sensu art 43.3 d).

- "El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados indicando asimismo la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario." (art 25.1)

- Los responsables de ficheros de información sobre solvencia patrimonial y crédito, cuando el afectado lo solicite, "le comunicarán los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección del cesionario." (art 28.2)

Deber de información al cesionario

- Deberá notificar a los cesionarios las rectificaciones o cancelaciones que se hubiesen efectuado en los datos cedidos (art. 15.3).

Deber de cooperación con la Agencia de Protección de Datos.

- Cumplir las instrucciones dictadas por el Director de la Agencia de Protección de Datos y proporcionar la información que éste solicite (art. 43.2 b).

- Remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquélla a tales efectos. (art. 43.3 i).

- No obstruir el ejercicio de la función inspectora (art. 43.3 j).

- El responsable del fichero estará obligado a permitir el acceso a los locales en los que se hallen los ficheros y los equipos informáticos previa exhibición por el funcionario actuante de la autorización expedida por el Director de la Agencia (art. 28.2 del Estatuto).

Establecimiento de Códigos-tipo

Los responsables de los ficheros de titularidad privada mediante acuerdos sectoriales o decisiones de empresa "podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto de los principios y disposiciones de la presente ley y sus normas de desarrollo."(art. 31).

Estos códigos tienen el carácter de códigos deontológicos o de buena práctica profesional y por tanto sólo vinculan al colectivo que previamente los ha aceptado.

Antes de la puesta en funcionamiento del Registro General de Protección de Datos, donde es preceptivo depositar o inscribir dichos códigos, la Asociación Española de Marketing Directo ya ha confeccionado un código tipo al que quedan sometidas todas las empresas miembros de dicha Asociación.

Estos deberes que hemos enunciado: seguridad de los datos, secreto profesional, rectificación y cancelación de datos personales, indemnización, información al afectado y al cesionario y cooperación con la Agencia de Protección de Datos obligan al responsable del fichero principalmente frente al afectado y a la Agencia de Protección de Datos.

Pero el responsable del fichero con independencia de estas obligaciones tiene unas funciones de gran importancia como son decidir sobre la finalidad, contenido y uso del tratamiento.

Como claramente se desprende de todo lo anterior la figura adquiere gran relieve y en su cometido se entremezclan funciones propias de un titular del fichero, sujeto obligado en el proyecto italiano, con labores propias de un responsable del tratamiento o del fichero propiamente dicho. La delimitación en la práctica de las funciones de uno y otro a veces no es tan fácil fijarla.

Perfil del responsable según la ley.

La LORTAD, a diferencia del Proyecto de Ley de Protección de Datos italiano de LOSANO, no especifica las condiciones que debe reunir el candidato a responsable del fichero, ni tampoco describe en un solo artículo, como se hace en el Proyecto italiano, las funciones del mismo.

Tanto los requisitos que debe cumplir el candidato como las funciones del puesto han de ser descubiertos a través de la lectura de la Ley.

Las funciones, en cierto modo, las hemos puesto de relieve en el punto anterior, por lo que en éste sólo nos referiremos a las características más importantes del perfil del responsable del fichero.

El responsable del fichero de datos de carácter personal según se desprende de su cometido descrito en diferentes artículos de la ley:

1) Debe tener experiencia y dotes organizativas.

2) Debe tener suficientes conocimientos informáticos.

3) Debe tener los conocimientos jurídicos necesarios para poder interpretar aplicar la LORTAD.

4) Debe depender directamente:

   En el caso de ficheros de titularidad pública del órgano ejecutivo correspondiente.
   En el caso de ficheros de titularidad privada de la dirección de la empresa.

5) Debe tener las suficientes dotes de diplomacia para mantener una cordial relación con la Agencia de Protección de Datos.

Vemos pues que el responsable del fichero ha de ser un profesional capacitado en ciertas áreas específicas, que en el organigrama de la empresa ocupará un lugar destacado dado el poder de decisión que tiene y que deberá estar en comunicación directa con la cúpula directiva.

Responsabilidades.

En el Considerando 24 de la Propuesta modificada de Directiva Comunitaria se dice: "que las legislaciones nacionales deben prever un recurso judicial para los casos en que el responsable del tratamiento no respete los derechos de los interesados; que los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el *responsable del tratamiento*, el cual sólo podrá ser eximido de responsabilidad si demuestra que ha adoptado las medidas de seguridad adecuadas; que deben imponerse sanciones disuasorias a cualquier persona ya sea de Derecho privado o de Derecho público, que no respete las disposiciones nacionales adoptadas en aplicación de la presente Directiva."

Posteriormente el texto modificado dedica el artículo 23 puntos 1 y 2 a tratar de la responsabilidad y su posible exoneración en la línea conceptual del considerando.

El artículo 42 de la LORTAD dispone:

"1.- Los responsables de los ficheros estarán sujetos al régimen sancionador establecido en la presente Ley.

2.- Cuando se trate de ficheros de los que sean responsables las Administraciones Públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 45, apartado 2."

Las responsabilidades en la LORTAD pueden ser de tres tipos: civil, penal y administrativo. A los dos primeros nos hemos referido anteriormente por tanto ahora estamos tratando de la responsabilidad administrativa.

La LORTAD en su artículo 42 personaliza la culpa administrativa en el responsable del fichero distinguiendo según se trate de ficheros de titularidad pública o privada.

No profundizaremos más en este tema que es objeto de otra ponencia y sí simplemente dejar constancia de la gran responsabilidad que recae sobre el responsable del fichero.

La LORTAD indudablemente ha seguido las directrices del Proyecto de Directiva Comunitaria cuando considera necesario que se impongan sanciones disuasorias.

Las sanciones previstas en la LORTAD son lo suficientemente disuasorias por lo elevado de sus importes.

Ahora quizás podamos comprender mejor esa inquietud personal de que hablábamos en la introducción.

Conclusiones.

El somero estudio realizado sobre la figura del responsable del fichero nos lleva a las siguientes conclusiones:

a) La demora en la promulgación de una ley de protección de datos en nuestro país ha incidido indirectamente en el retraso en la adopción de medidas de seguridad de los mismos en las empresas y en las Administraciones Públicas.

b) La contínua remisión a la vía reglamentaria para el desarrollo de su articulado crea un cierto grado de incertidumbre pues por esa vía se puede modificar lo dispuesto en la Ley.

c) La LORTAD ha creado alarma en los medios empresariales pues al no estar establecidas aún las condiciones de integridad y seguridad de los fiche-

ros automatizados ni la de los centros de tratamiento, locales, equipos, sistemas y programas pendientes de la aprobación del oportuno reglamento temen que sean muy severas y supongan importantes desembolsos económicos.

d) La inquietud detectada en ciertos ejecutivos viene dada por la ambigüedad y responsabilidad de la figura que aparece como el "chivo expiatorio" de la Ley.

e) En la mayoría de los ordenamientos jurídicos consultados, excepto en el Proyecto italiano comentado de LOSANO, existe un solapamiento entre las funciones del titular del fichero y las del responsable del mismo.

f) Existe, por parte del legislador, gran interés en que la identidad del responsable del fichero sea perfectamente conocida.

g) En la tarea del responsable del fichero se mezclan funciones directivas, técnicas, jurídicas, organizativas, representativas y puramente burocráticas.

h) La persona elegida para responsable del fichero ha de tener conocimientos informáticos y jurídicos así como dotes organizativas.

Por todo ello volvemos a insistir en la necesidad de prestar atención a la figura del responsable del fichero, tan importante para una correcta aplicación de la Ley y que en el futuro, a través de los reglamentos que faltan por aparecer y de las resoluciones de la propia Agencia de Protección de Datos, debe ser definida con mayor rigor.

Esperamos que estas modestas líneas se entiendan como lo que son, una simple llamada de atención sobre un tema que consideramos debe ser estudiado con mayor profundidad.

Legislación y Documentación.

*Ley Orgánica 5/1992 de 29 de octubre de Regulación del Tratamiento Automático de los Datos de Carácter Personal. BOE núm. 262 de 31 de octubre de 1992.

*RD 428/1993 de 26 de marzo por el que se aprueba el Estatuto de la Agencia de Protección de Datos. BOE núm. 106 de 4 de mayo de 1993.

*Propuesta modificada de Directiva del Consejo 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. Bruselas 15 de octubre de 1992. COM(92) 422 final. SYN 287.

Bibliografía Consultada.

Artículos

DAVARA RODRIGUEZ, MIGUEL ANGEL

*La Ley española de protección de datos (LORTAD): ¿una limitación del uso de la informática para garantizar la intimidad? (I) y (II). Actualidad Jurídica Aranzadi 12 y 19 noviembre 1992.

HEREDERO HIGUERAS, MANUEL

*La protección de los datos personales registrados en soportes informáticos. Actualidad Informática Aranzadi núm.2. Enero 1992.

*La protección de datos en los Servicios de Telecomunicaciones: El Proyecto de Recomendación del Consejo de Europa. Tecnologis núm. 11. Abril-Junio 1992.

PAEZ MAÑA, JORGE

*La incidencia de la LORTAD en los procesos de producción y distribución de ficheros. Actualidad Informática Aranzadi núm. 7. Abril 1993.

PESO NAVARRO, EMILIO DEL

*La LORTAD. Breve apunte a un Proyecto de Ley. Base Informática núm. 21 noviembre 1992.

Ponencias

ALVAREZ CIENFUEGOS SUAREZ, JOSE MARIA

*El derecho a la intimidad personal, la libre difusión de la información y el control del Estado sobre los Bancos de Datos. Encuentros sobre Informática y Derecho 1990-91. Facultad de Derecho e Instituto de Informática Jurídica. ICADE. Universidad Pontificia de Comillas. Aranzadi. Pamplona 1992.

CARRASCOSA LOPEZ, VALENTIN

*Derecho a la Intimidad Informática. Revista Informática y Derecho núm. 1.UNED. Mérida 1992.

DAVARA RODRIGUEZ, MIGUEL ANGEL

*Normativa para la Protección de la Intimidad. Planteamiento general. Implicaciones socio-jurídicas de las Tecnologías de la Información. IX Encuentro 1991. Citema Madrid 1992.

LOPEZ-MUÑIZ GOÑI, MIGUEL y RODRIGUEZ ARRIBAS

*Infracciones y sanciones en la Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. 5° Congreso internazionale sul tema: Informática e attivitá giuridica. Corte Suprema di Cassazione. Roma mayo 1993.

LOSANO MARIO G.

*Para una Teoría General de las Leyes sobre Protección de Datos Personales. Implicaciones socio-jurídicas de las Tecnologías de la Información IX Encuentro 1991. Citema Madrid 1992.

OROZCO PARDO, GUILLERMO

*Notas acerca del "Derecho de acceso" recogido en el Proyecto de Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal. Actas III Congreso Iberoamericano de Informática y Derecho. UNED. Centro Regional de Extremadura. Mérida 1992.

PEREZ LUÑO, ANTONIO ENRIQUE

*Panorama general de la Legislación española sobre protección de datos. Implicaciones socio-jurídicas de las Tecnologías de la Información. IX Encuentro 1991. Citema. Madrid 1992.

*Del Habeas Corpus al Habeas Data. Encuentros sobre Informática y Derecho 1990-91. Facultad de Derecho e Instituto de Informática Jurídica ICADE de la Universidad Pontificia de Comillas. Aranzadi. Pamplona 1992.

Obras

*Informática Leyes de Protección de Datos (I)
Documentación Informática núm. 2. Presidencia del Gobierno. Secretaría General Técnica. Madrid 1977.

*Informática Leyes de Protección de Datos (III).
Documentación Informática núm. 4. Ministerio para las Administraciones Públicas. Madrid 1988.

CONESA MADRID, FULGENCIO

*Derecho a la intimidad, informática y estado de derecho. Universidad de Valencia. Valencia 1984.

DAVARA RODRIGUEZ, MIGUEL ANGEL

*Derecho Informático. Aranzadi. Pamplona 1993.

LOSANO, MARIO G., PEREZ LUÑO, ANTONIO ENRIQUE Y GUERRERO MATEUS, MARIA FERNANDA.

*Libertad Informática y Leyes de Protección de Datos Personales. Cuadernos y Debates núm. 21. Centro de Estudios Constitucionales. Madrid 1989.

LUCAS MURILLO, PABLO

*El derecho a la autodeterminación informativa. Temas Clave de la Constitución española. Tecno. Madrid 1990.

TELLEZ VALDES, JULIO

*Derecho Informático. Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas. México 1987.

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.

I) 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[1], 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 L6pez
El Defensor del Pueblo: ¿factor de democratización?. Revista Juridica 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. 1980, 345.
-Victor Fairén Guillén.
Normas y notas sobre el "Ombudsman" de Suecia. Revista de Estudios Políticos. num. 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[2].

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 Viñas 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 Mº de Justicia nums. 1507-1508, 25 Octubre y 5 Noviembre, 1988.

■ 2 La Ley 36/1985 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: Sindic 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 deber 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 util.
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 Aministración, 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 aleman -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 ningun 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 esta 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 Constitucion 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 dimanan 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[3]. 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

■ 3 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 limites 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.*" [4]

En nuestros días una de las cuestiones mas 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 traves del control del interesado en relación con el acceso de otros a la información más personal, a los datos mas reservados de cada uno.[5]

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 231/1988 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[6], 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[7], 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 land 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 (Bundesgesetzblalt 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, ulteriormente 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, nº 565), Canadá (Privacy Act. 1982), Dinamarca (Ley 8 de junio de 1978, nº 293, sobre los registros privados y Ley 8 de junio de 1978, nº 294, sobre los registros de la Administración pública), Gran Bretaña (Ley 12 julio 1984)[8] , Islandia (Ley nº

■ 8 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, nº 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, nº 48), Suecia (Ley 11 mayo 1973, nº 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 reqistrar y su puesta al día deben estar asequradas. (Seguridad y calidad de la información; Actualización de datos).

-Deben precisarse *los fines del reqistro* 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 solicitados, 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 reqistradas 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 Comite 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 Unica 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[9]. 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[10] 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 60/75.
■ 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[11] 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[12] 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[13]. 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.[14]

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[15], 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[16].

- Una propuesta de decisión en el ámbito de la seguridad de los sistemas de información.[17]

- Una propuesta de reglamento relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico[18].

- 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 Eurooeo y las actividades de la Comunidad Europea*, Parlamento Europeo, Dirección General de Estudios (1988), 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[19] y la propuesta de reglamento relativo a la transmisión de informaciones estadísticas[20].

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 proteccion de las personas físicas en lo que respecta al tratamiento de datos Personales y la libre circulacion de estos datos.[21]

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 159/30 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 segun 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"[22] del artículo 2, a la luz del desarrollo de la automatización y de las telecomunicaciones, así como la definición de "tratamiento de datos personales"[23] 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 fsicas. 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 traves 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 cooperacion policial en bases de datos nacionales conectadas por medio de un sistema central que se encuentra hoy en La Haya, dependientes del Ministerio holandes 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 deberan 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"[24], 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."[25]

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 bid.

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 ejecucion de la tarea legal consignada en la descripcion 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[26], 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 standares 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 informacional 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 qeneral 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 salvaquardia 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.

Segun 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 divulqado;* 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 ileqítimas 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[27].

VII) La Ley Orgánica 5/1992 de 31 de Octubre de 1992 sobre Protección de Datos Personales y su posible Inconstitucionalidad.[28]

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 Diritto. Junio-Abril 1989.
-"L'Informatique au service du juriste", de Henri Manzanares y Philippe Nectoux. Litec, Librairies Techniques, 1987).

■ 28 Ver, entre otros, los trabajos publicados en las Actas del 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 Santamaria Ibeas.
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 Deninger. Problemas Actuales de la Documentación y la 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 Constitucion española, recurso que se fundamentó en lo siguiente:

PRIMERO. Inconstitucionalidad del artículo 19.1 de la Ley Orqanica 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 proteccion 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 parrafo del art. 22.2 de la Ley Orqánica 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 iqual 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 obtencion 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 tendra la obligacion 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 razone pblico o ante intereses de terceros más dignos de protección"[29] .

En nuestra opinión, las restricciones establecidas en los párrafos entrecomillados 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 ni 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[30].

■ 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.

La Abogacía y la L.O.R.T.A.D.

JOSEP JOVER I PADRO
Diputado de la Junta de Gobierno
del Colegio de Abogados de Barcelona.

Introducción

CONSIDERACIONES PREVIAS: como funciona la Técnica del rastrillo,

Las nuevas situaciones internacionales derivadas del Convenio para la Protección de las Personas con respecto al tratamiento de datos personales firmado en Estrasburgo en 1981, los acuerdos de Schenguen y la propuesta de directiva del Consejo de la Comunidad Europea relativa a la protección de las personas en lo que hace referencia a los datos personales, fuerzan al ministerio correspondiente a intentar regular los derechos y obligaciones de los agentes intervinientes en la producción y distribución de información codificada.

La catarsis cuaja en la Ley Orgánica 5/1992 de 29 de Octubre, de regulación del tratamiento de datos de carácter personal.

La verdad es, que el legislador ha querido hacer, en la forma, una Ley tan completa y tan perfecta, que la misma ha nacido muerta. Ha nacido muerta, porque recuerdo, la obligación de inscribir las bases de datos fine el 30 de enero de 1994, afecta de golpe a cientos de miles de bases de datos, y aún no se ha empezado a trabajar en ningún sentido.

La obligación de inscribir afecta a todas las bases Españolas, pequeñas o grandes, con la excepción de las de la Administración, las propiedad de las personas físicas, no jurídicas, con fines exclusivamente personales, y las de partidos políticos, sindicatos, iglesias y los dedicados a estadística. (Vide Art. 2 de la Ley)

El ficherito en dbase que pueda tener el último viajante de jamones, el sastre con las medidas de sus clientes, el profesor de sus alumnos, la relación de nóminas de mi despacho, o el fichero de facturación de un minorista de venta de azulejos. Todos ellos son obligados a declararlos.

Además, la titularidad del fichero la adquiere de forma originaria el creador del mismo, y es sobre este titular inicial quien cabe la obligación de comunicar a la Agencia la existencia y la finalidad del fichero, el tipo de datos que se pretenden recopilar y el procedimiento de recogida de los mismos, su estructura, las medidas de seguridad a adoptar sobre el mismo, las cesiones que se prevean realizar y el nombre de las personas y órganos responsables de su utilización así como las de registrar el fichero en la forma que reglamentariamente se determine.

Nace muerta, porque además toda la información de cada una de las bases y sus modificaciones es físicamente impublicable. La agencia de protección de datos no tendrá ni bastante dinero ni bastantes empleados para controlar y publicar en un catálogo esos cientos de miles de bases de datos, como es su obligación según la LORTAD.

Nace muerta por que no tiene en cuenta la cantidad de bases de datos con vigencia transitoria, o duración limitada. p. ej. la base de datos que se crea para estas jornadas ni tampoco tiene en cuenta la cantidad de modificaciones el los campos que pueden tener esos ficheros o bases de datos de alcance limitado.

Llega tanto a querer precisar y encajonar, que con una lectura atenta del art. 24 del Reglamento que desarrolla la Ley Orgánica, es que no se salva ni el ficherito que tiene mi hija de sus amigas, en el que consta el nombre y la dirección.

Nace muerta porque no va a evitar la existencia de paraísos de datos, en la vida tendrá tanto presupuesto como sus datractores, médicos y productos farmacéuticos, tampoco regula la importación de datos personales, lo que quiere decir que se exportan datos inocuos, se cruzan, se convierten en sensibles y después se importan.

Y nace muerta, finalmente, porque esa especie de supermán con derecho a penetrar en puertas y domicilios ajenos, que será el funcionario inspector de la Agencia (Art. 28 del Reglamento) o no va a encontrar nada, o va a tener que trabajar, si quiere resultados, de la mano del juez y de la Policía Judicial.

Para que va a servir, pues para poder demandar por daños y percjucios a los titulares de ficheros privados (Art. 17 - 5, porque la demandas a la Administración, bien solo cabe recordar que la administración es inembargable.

I.- La abogacía como profesión que conoce y trata datos sensibles. Responsabilidad de sobre los ficheros. Medidas de seguridad.

Una de las sorpresas que como abogado tuve al hojear por primera vez el texto de la L.O.R.T.A.D. fue el de ver que el legislador había olvidado absolutamente a los profesionales del Derecho. Dedica todo un artículo, específicamente el artículo 8, a desarrollar la filosofía sobre los datos que afectan a la salud, habla de las obligaciones y derechos que tienen médicos y hospitales, pero, los profesionales que tratamos de la "salud social" del individuo, parece que la ley no piense en regularnos. Sólo en el apartado 5º del Artículo 7º sale un pequeño párrafo que dice. "Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros automatizados de las ADMINISTRACIONES PUBLICAS competentes, en los supuestos previstos en las respectivas normas reguladoras."

Estrictamente pues, vemos que el artículo está pensado para permitir el funcionamiento del Registro de Penados y Rebeldes y nuestras "amigas", RITA, BERTA y también EL DUQUE DE AHUMADA. Para poder efectuar cruces de información entre las bases de datos de las Administraciones permite el Artículo 19 de la Ley un desarrollo reglamentario que cubre cualquier contingencia.

Pero es que lo que el legislador no ha pensado es que existen una serie de instituciones y profesionales, a caballo entre lo público y lo privado, que tratan cada día con esos datos sensibles, y por tanto, no es de extrañar que aparezcan esos datos en los ficheros de Colegios profesionales y profesionales como, Abogados, graduados sociales, asesores tributarios, gestores, (las multas son sanciones administrativas), ...

Estrictamente pues, estamos excluidos de facto de la LORTAD; no podemos llevar una base de datos eficaz, porque ésta contiene datos susceptibles de protección.

Gracias a Dios, el abogado aun tiene la cláusula de secreto profesional y puede negarse a contestar lo que tiene èn su base de datos.

Pero la realidad es muy otra, los juristas tenemos y tendremos en nuestras bases de datos ítems sensibles. Eso es un problema y no podemos obviarlo.

Hablemos antes que nada de la figura del responsable del fichero. La LORTAD afecta tanto a los agentes tradicionales del proceso informativo automatizado (creadores de los archivos y productores, distribuidores y receptores de la información nominativa), como las personas físicas y jurídicas que por cuenta de terceros presten servicios de tratamiento automatizados de datos de carácter personal, y sobretodo a los titulares de los ficheros o archivos automatizados que contengan información nominativa y a los responsables de los mismos.

Es la persona física, en fin, la que tiene la máxima responsabilidad sobre los datos introducidos, El Administrador único, el Presidente, ...salvo que se haya delegado expresamente en otra persona física, entendemos incluso que cuando se hace la remisión a órganos se hace a los jefes de dichos órganos.

Esto quiere decir que queda enmarcada claramente en el caso en que nos ocupa, al abogado como responsable único de sus bases de datos, al igual que el Decano lo es de la base de datos de la corporación, a no ser que se haya delegado en una tercera persona.

Se plantea además de que todos los ficheros que afecten a nuestra profesión tengan mecanismos físicos e informáticos que los protejan de los extraños. El Abogado o la corporación son absolutamente responsables de la circulación indebida de los datos de su fichero

El secreto profesional del abogado es un secreto de pasado. Es decir jamás puede proteger el secreto profesional, sobretodo en el ámbito penal, una acción de futuro. Es por ello que el abogado debe proteger la información del pasado.

II.- Bases de datos excluidas.

Para nuestro interés, solo podemos considerar como excluidas las bases de datos de contenido científico. Legislación y normativa, jurisprudencia y doctrina. Sean las que edita el propio Estado, como las recopiladas por empresas privadas para su distribución como las que se puedan disponer en un despacho como jurisprudencia propia.

Los Ficheros de informática jurídica han de cumplir un sólo requisito. El no poder vincular personas con fundamentos de derecho.

La regulación la encontramos en el art. 2 de la propia ley donde relaciona exhaustivamente las excepciones a la inscripción.

III.- Bases de datos específicas de los profesionales de la abogacía:

- Ficheros derivados de los programas de gestión del despacho. Principalmente son tres El fichero de clientes, el fichero de asuntos y el fichero económico. En los tres se manejan datos sensibles que relacionan los asuntos llevados, la fiabilidad y la capacidad de pago de los clientes, junto con las incidencias procedimentales.

- Ficheros de contenido económico. Existen otros ficheros que el abogado también consulta, y estos son los de morosos. La Regulación parte del Art. 28 de la propia Ley. Es obligación del fichero y de su responsable comunicar los sus datos al afectado, habiendo una limitación en el histórico de seis años.

El problema surge por la propia operativa bancaria. Al haber desaparecido en 1990 el REGISTRO DE ACEPTOS IMPAGADOS, han sido creadas por bancos, cajas y sociedades de instrumentos de crédito, corporaciones conjuntas de tratamientos de datos económicos de los clientes, los cuales, no sólo afectan a la morosidad sino que radiografían la capacidad económica del cliente.

Estas sociedades están en cierta manera fuera de control de los bancos y clientes.

Hay algunos Registros específicos de morosidad. Normalmente son utilizados a través de Agencias de informes o de detectives. El problema aquí surge del choque entre la LORTAD y la Ley de Seguridad Privada, Quien obliga en su Art. 2 4º a lo siguiente: "Asimismo, las empresas de seguridad y los

detectives privados presentarán cada año un informe sobre sus actividades al Ministerio del Interior, que dará cuenta a las Cortes Generales del funcionamiento del Sector. Dicho informe habrá de contener relación de todos los contratos de prestación de servicios de seguridad celebrados con terceros, con indicación de la persona con quien se contrató, y de la naturaleza del servicio contratado, incluyéndose además los demás aspectos relacionados con la Seguridad pública, en el tiempo y la forma que reglamentariamente se determinen". Se rompe aquí toda confidencialidad, dándose la paradoja que quien queda "retratado" no es sólo el que está dentro del fichero sino también quien pregunta.

IV.- La obligación de declarar e inscribir.

De lo Anteriormente expuesto vemos que hay una parte de los ficheros de los abogados que es factible inscribir, la que corresponde a la gestión de sus asuntos. Las otras quedan, per se, fuera del campo de la ley, y por tanto su única regulación será la que afecta al Secreto Profesional, recogida de un modo genérico en la propia Constitución y específica en el Estatuto General de la Abogacía (Art. 41), Art. 360 del Código penal, Estatutos colegiales y en la Recopilación de Usos y Costumbres de la misma. Es defendible la no inclusión por ser el Derecho de defensa una obligación de rango superior, que afecta específicamente a los Abogados.

VI.- Los colegios de abogados.

Los colegios profesionales están a caballo entre el Derecho Público y el Privado. Tampoco se ha pensado en ellas. Podemos definir tres grandes grupos de bases de datos.

- Bases de datos administrativas La General, la de la Mutualidad, Bolsa del Trabajo, la de las empresas oferentes de trabajo, Registro de Despachos colectivos, Registro de convenios entre despachos.

- Bases de datos de deontologia e intrusismo.

- Bases de datos del turno de oficio, y asistencia al detenido. Registro de reconocimiento de firmas, Registro de Habilitaciones.

VII.- La elaboración de un código tipo para los colegios de abogados y los abogados españoles.

Por todo lo visto, tendrá que jugar un papel fundamental en la conducta de los profesionales, técnicos y Colegios profesionales.

Decía Casanova que "el veneno en manos del sabio es medicina, mientras que la medicina en manos del necio, es veneno". Este agudo aforismo es aplicable a casi cualquier profesion. Ahora nos hemos dado cuenta de los efectos nocivos de la informática concebida como instrumento, pero debemos recordar que las profesiones más antiguas, como los médicos y Abogados, profesiones que juegan con la vida y la honra de las personas, contamos con estrictos códigos deontológicos bien definidos. Los médicos desde Hipócrates, los Abogados desde la Ley de las XII tablas

Ahora bien, quizá lo que valga la pena es apostar por un "PACTO ETICO", la LORTAD, lo llama sencillamente código tipo, donde corporaciones y profesionales utilicen razonablemente (es decir en el legítimo quehacer de su función profesional) sus bases de datos, donde no existan más datos que los necesarios para llevar a cabo su labor.

Quizá la mejor definición de este pacto ético sea el Párrafo primero del Art. 4 de la LORTAD que exige que los datos recogidos sean adecuados, pertinentes y no excesivos en relación al ámbito y a las finalidades finalistas legítimas de las bases.

Siete son las obligaciones del Abogado o del colegio para con sus ficheros.

MANTENER AL DIA LA BASE DE DATOS, permitiendo la retirada de los datos inútiles y obsoletos y actualizando los datos que el ella figuren.

OBTENCION Y MANIPULACION CORRECTA DE LOS DATOS. El cliente ha de ser consciente de la emisión de sus datos personales para la base, de qué se hará con ellos y de que éstos nunca se utilizarán en perjuicio suyo.

DERECHO A CONOCER. El cliente tiene derecho a conocer en cada momento la cantidad y calidad de los datos que tiene la base, no sólo eso sino que además tiene el derecho a conocer, que datos van a quedar en el fichero una vez haya acabado su asunto.

DERECHO DE RECTIFICACION. De los datos, comentarios y opiniones, que figuren en la base y que esta rectificación sea efectiva.

LA ACEPTACION DE UNAS NORMAS ETICAS DE SECRETO del personal que manipula la base. Si bien el máximo responsable es el abogado el secreto afecta a todos sus colaboradores. Estas normas éticas de secreto se añaden a las propias del secreto profesional de los abogados. Debemos entender, y es importante que se sepa, que el secreto profesional de los abogados no solo afecta a los documentos que pueda haber dentro de un expediente, sino a todos los archivos y ficheros sean de base de datos, sean de tratamiento de textos que pueda poseer y que hagan relación a su ejercicio profesional.

SEGURIDAD FRENTE A LOS INTRUSOS. El responsable de la base de datos está obligado a proteger física e informáticamente sus ficheros del acceso de terceras personas no autorizadas.

SEGURIDAD EN LA REVELACION ESTADISTICA. No debemos olvidar que el jurista es un científico, los resultados de la revelación estadística de la base deben proteger la personalidad de sus clientes, asegurándose de que en ningún caso se puedan vincular asuntos con clientes.

El Movimiento Internacional de Datos en la Ley Española de Protección de Datos

SANTIAGO RIPOLL CARULLA

Profesor-Titular de Derecho Internacional de la Facultad de Derecho de la Universidad Pompeu-Fabra.

Introducción.

1. El Título V de la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal (L.O.R.T.A.D.) dedica los dos artículos que lo componen a la ordenación del "Movimiento Internacional de Datos" (arts. 32 y 33)[1].

Pese a la brevedad con que la trata, el mero hecho de que la Ley haya dado autonomía a la cuestión del movimiento internacional de datos es reflejo de la importancia de la misma. "El libre flujo de los datos personales constituye -según indica el preámbulo de la Ley- una auténtica necesidad de la vida actual de la que las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional pueden ser simples botones de muestra".

■ 1 Ley Orgánica 5/1992, de 29 de octubre. BOE, núm 262, de 31 de octubre de 1992.

Con la incorporación de esta ordenación, el derecho español comienza un proceso recogido explícitamente por la normativa internacional existente en la materia. Es por ello que el presente artículo se estructura en dos partes claramente diferenciadas: una primera, centrada en el estudio de la normativa internacional, y en cuyo marco se analizará especialmente la normativa comunitaria sobre la cuestión tanto por tratarse del texto más recientemente elaborado como por el carácter vinculante que le acompañará; una segunda, dedicada al análisis de la ordenación contenida en la LORTAD.

I. La Regulación Jurídico-Internacional del "Movimiento Internacional de Datos"

A) El principio del "nivel de protección equivalente"

2. Aunque el cuerpo de normas jurídico-internacionales específicamente dedicados a la ordenación de la protección de los datos personales no es extenso, de entre el mismo merecen destacarse los cuatro textos que abordan esta ordenación de un modo general, a saber, los Principios de las Naciones Unidas (1990)[2], las Líneas Directrices de la OCDE (1980)[3], el Convenio del Consejo de Europa (1981)[4], y la propuesta de Directiva de la Comunidad (1992)[5].

Las diferencias entre unos y otros son numerosas, dado que poseen ámbitos de aplicación diferentes y grados de obligatoriedad distintos. Por otra parte, como es sabido, la Directiva de la Comunidad aún no ha entrado en vigor, ni siquiera.

En cualquier caso, de entre los elementos comunes a todos estos textos, conviene señalar que en todos ellos se regula la cuestión del "movimiento internacional de datos" como cuestión autónoma, otorgándosele, en líneas generales, una ordenación unívoca.

- 2 COMISION DE DERECHOS HUMANOS, *Los Derechos humanos y el progreso científico y tecnológico. Versión revisada de los principios rectores para la reglamentación de los ficheros computarizados de datos de carácter personal*, E/CN.4/1990/72, 20 de febrero de 1990.
- 3 OCDE, *Recommendation du Conseil concernant les Lignes Directrices régissant la protection de la vie privée et les flux transfrontières des données de caractère personnel*, 23 septembre 1980.
- 4 *Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal*, hecho en Estrasburgo el 28 de enero de 1981. Ratificado por España por Instrumento de 27 de enero de 1984. *BOE*, DE 15 DE NOVIEMBRE DE 1985.
- 5 *Propuesta modificada de Directiva del Consejo 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*, Doc. COM (92) 422 final - SYN 287, de 15 de octubre de 1992.

3. La solución jurídica arbitrada por el Derecho internacional a la cuestión del movimiento internacional de datos pasa *grosso modo* por considerar que entre dos países afectados por un flujo de datos a través de sus fronteras, la información deberá circular tan libremente como en el interior de cada uno de los territorios respectivos, siempre y cuando el nivel de protección otorgado al individuo en cada uno de los ordenamientos afectados sea similar.

En rigor, la exigencia de tal homogeneidad se realiza a través de una terminología diversa, ya que mientras en algunas ocasiones se prescribe que "la legislación de los países afectados (...) ofrezca garantías comparables de protección de la vida privada" (Principio 9 de las Naciones Unidas), en otros casos se exige que "el tercer país de que se trate garantice un nivel de protección adecuado" (Art. 26.1 de la propuesta de Directiva).

En última instancia, resulta claro que para el legislador internacional, la posibilidad de las transmisiones internacionales de datos se hace depender de un criterio valorativo, al que se trata de modular por una doble vía: de una parte, objetivándolo al máximo; de otra, permitiendo la diversificación de las autoridades que deberán adoptar tal decisión.

B) Modulaciones al principio

4. En relación a la primera cuestión, conviene retener especialmente la ordenación recogida en la propuesta de Directiva, cuyo artículo 26.2 precisa los elementos que deben tenerse en cuenta para evaluar la idoneidad de la protección ofrecida por el país tercero. "Se trata - indica - de todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en concreto, la naturaleza de los datos, el fin o los fines del tratamiento o de los tratamientos previstos, o la normativa vigente en el país en cuestión". A este respecto, resultará oportuno examinar la normativa general o sectorial, su aplicación real, así como las normas profesionales en vigor, recogidas en los códigos de conducta correspondientes. En opinión de Blume, en la práctica será determinante que el tercer país posea una legislación sobre protección de datos que se refiera tanto a los bancos de datos de titularidad pública como a los privados, pues ésta es una condición que varía sensiblemente de una legislación a otra. En este sentido, también resultará importante valorar si el país tercero contempla la protección de los datos referentes a personas jurídicas, y, en última instancia, será especialmente útil considerar si el país en cuestión ha ratificado o no la Convención del Consejo de Europa sobre la materia.

5. Por lo que se refiere a la instancia de decisión, conviene señalar que, de acuerdo con la propuesta de Directiva, es competencia de los Estados miem-

bros el evaluar la idoneidad de la protección y decidir, en su caso, la prohibición de la transmisión. Si tal es su decisión, los Estados miembros deberán informar a la Comisión, la cual comprobará, a su vez, tal extremo.

En caso de que efectivamente compruebe que el tercer país "no garantiza un nivel de protección adecuado y que la situación que de ello se deriva es perjudicial para los intereses de la Comunidad o de un Estado miembro, podrá entablar negociaciones con vistas a corregir esta situación".

En cualquier caso, de acuerdo con el artículo 27 de la propuesta de Directiva, es posible que el Estado miembro autorice la transmisión de los datos aun a sabiendas de que el nivel de protección previsto en el ordenamiento jurídico del Estado receptor de los datos no es el adecuado. Para que ello sea posible es preciso que "el responsable del tratamiento aduzca motivos suficientes que resulten, en particular, de disposiciones contractuales apropiadas que garanticen, en especial, el ejercicio efectivo de los derechos de los interesados", Como es lógico, también en este caso deberá el Estado miembro notificar tal autorización a la Comisión, que, tras examinar los términos del contrato en cuestión, incluso podrá prohibir la transmisión o supeditarla a condiciones complementarias.

Por otra parte, como es fácilmente imaginable, la Comisión podrá decidir que el tercer país en cuestión garantiza el nivel de protección equivalente [6].

C) Régimen de excepciones

6. En fin, conviene señalar que la normativa internacional prevé la posibilidad de recoger excepciones al principio desarrollado previamente, de modo que, en determinadas ocasiones, sea posible transmitir datos personales a terceros países que no cuenten con un grado adecuado de protección.

De acuerdo con el artículo 26, apartado primero, de la propuesta de Directiva, ello será posible:

- cuando el interesado haya dado su consentimiento, bien de un modo expreso, bien a través de una cláusula contractual. "En tales casos, el

■ 6 La práctica seguida en el marco del Convenio del Consejo de Europa no está lejana a la comunitaria: el Comité Consultivo creado por el Convenio de 1981 ha elaborado un documento que sistematiza los sistemas reales empleados por cada Estado parte al momento de fijar el criterio de equivalencia.

interesado debe estar informado (...), de modo que pueda decidir si quiere arriesgarse o no a que se lleve a cabo la transferencia en cuestión" [7] ;

- cuando resulte necesaria para la salvaguarda de un interés público importante o del interés vital del interesado. "El objetivo de estas excepciones es facilitar la cooperación internacional (por ejemplo, en la lucha contra el blanqueo de capitales o para el control de las entidades financieras) o posibilitar la transferencia de datos médicos en circunstancias en que el interesado no puede expresar su voluntad" [8] .

II. El Movimiento Internacional de Datos en la LORTAD.

7. Como ha sido indicado previamente, los artículos 32 y 33 de la LORTAD afrontan la ordenación del movimiento internacional de datos.

En líneas generales, esta normativa se caracteriza por su simetría con la normativa internacional sobre la cuestión, tal y como, por cierto, reconoce el propio legislador en el preámbulo de la Ley: "En este punto - señala -, la Ley traspone la normativa contenida en el artículo 12 del Consejo de Europa". Con esta trasposición - se indica algunas líneas más adelante -, "no sólo se cumple con una exigencia lógica, la de evitar un fallo que pueda producirse en el sistema de protección a través del flujo a países que no cuentan con garantías adecuadas, sino también con las previsiones de instrumentos internacionales como los Acuerdos de Schengen o las futuras normas comunitarias".

En consecuencia, pues, la lógica jurídica de la ordenación recogida en la Ley española es *mutatis mutandi* idéntica a la que caracterizaba la normativa internacional sobre esta cuestión, de modo que también es posible distinguir en la misma un principio general, modulado por circunstancias especiales, y acompañado por determinadas excepciones.

Esta simetría se extiende incluso a aquellos aspectos de la normativa internacional que han merecido una solución menos afortunada, siendo así, por ejemplo, que al igual que la Convención del Consejo de Europa, la LORTAD únicamente contempla el supuesto de exportación de los datos personales, sin considerar, por consiguiente, la posibilidad de una importación de los mismos.

■ 7 *Propuesta modificada de la Directiva del Consejo 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* (Exposición de motivos), Doc. COM (92) 422 final SYN 287, Bruselas, 22 de octubre de 1992. pág. 36.

■ 8 *Ibid.*, pp. 36-37.

Esta omisión resulta ciertamente criticable pues puede comportar ciertas incongruencias, tal como ilustran J. Piñol y O. Estadella en referencia al Convenio 108 del Consejo de Europa: cuando el Estado exportador de datos personales aun no automatizados no sea parte del Convenio del Consejo de Europa y el receptor sí lo fuera, podría darse la paradoja de que el Estado receptor, una vez haya efectuado el tratamiento automatizado, tuviera que negarse, dadas sus obligaciones convencionales, a reexportarlas al Estado de origen, porque éste no tiene una protección equivalente.

Por lo demás, la falta de rigor en la terminología empleada es buena prueba asimismo del nivel de mimetismo característico de la normativa española.

A) El "nivel de protección equiparable" como principio general aplicable

8. De acuerdo con el artículo 32 de la LORTAD, "no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley".

En simetría, pues, a la normativa internacional, la LORTAD exige la similitud en los ordenamientos afectados como principio básico para posibilitar la transmisión de datos personales recogidos en España a países terceros.

Y, tal como se ha señalado previamente, en simetría asimismo con la normativa internacional, la Ley española exige tal semejanza mediante el recurso a una terminología diversa, poco rigurosa, de modo que, de acuerdo con la misma, es suficiente que exista un nivel de protección "equiparable", y no ya un grado de protección "equivalente". En opinión de J.L. Piñol y O. Estadella, el recurso a esta terminología podría conllevar un nivel de exigencia menor por parte de las autoridades españolas al momento de autorizar o prohibir las transmisiones de datos a terceros países, aunque, en cualquier caso, la solución establecida en la LORTAD no difiere en exceso de la arbitrada por el Derecho internacional, ya que en ambos casos se hace depender la autorización o prohibición de la transmisión de un criterio valorativo que, también en el caso español, aparece parcialmente modulado.

B) Modulaciones al principio

9. A diferencia de los establecidos en la propuesta de Directiva comunitaria, pero en concordancia con el Convenio de 1981, la LORTAD no esboza los elementos que deberían atenderse al momento de evaluar la idoneidad de la protección ofrecida por el país destinatario de la transmisión.

Con todo, esta circunstancia, y en particular su principal consecuencia - la falta de objetividad - se ve parcialmente mitigada gracias a la condición de Estado parte en el Convenio y a los trabajos emprendidos al efecto por el Comité Consultivo constituido por el mismo. De forma similar, los elementos valorativos reseñados en la propuesta de Directiva y que serán desarrollados por los órganos de control previstos en la misma, informarán a los responsables de los bancos de datos y a las autoridades españolas.

10. De acuerdo con la legislación española, la autorización o prohibición de la transferencia internacional de datos compete en primera instancia al responsable del fichero, ya que él es quien ha de valorar sobre la finalidad, contenido y uso del tratamiento de los datos (entendiéndose por éste todas aquellas "operaciones y procedimientos técnicos (...) que permitan la recogida, grabación, conservación, elaboración, modificación, bloque y cancelación, así como las cesiones de datos que resulten comunicaciones, consultas, interconexiones y transferencias") [9].

Ahora bien, la Agencia de Protección de Datos es la única competente para "ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos" (Art. 36.1). Esta potestad se extiende hasta el extremo de reconocérsele la posibilidad de autorizar una transmisión de datos a un tercer país que no cuente con un nivel de protección equiparable. Para ello será menester una autorización previa del Director de la Agencia, "que sólo podrá otorgarla si se obtienen garantías adecuadas" (Art. 32 in fine) [10].

C) Excepciones al principio

11. El artículo 33 de la LORTAD prevé ciertas excepciones a la norma general sobre las transmisiones internacionales de datos. En líneas generales, los supuestos contemplados son subsumibles en las categorías diferenciadas

- 9 Art. 3 "Definiciones", letras d), "Responsable del fichero", y c) "Tratamiento de datos", respectivamente.
- 10 En concordancia, así, con el artículo 12.2, letra d) del RD 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, BOE, de 4 de mayo de 1993.
  Ver también los artículos 25 y 26 del mismo texto legal, en los que se señala que tales autorizaciones se inscribirán en el Registro General de Protección de Datos y que corresponde a este órgano la instrucción de los expedientes de autorización de las transferencias internacionales de datos.

en relación a las excepciones previstas en la normativa internacional y comunitaria -para la salvaguarda de un interés público importante o del interés vital del interesado-, si bien es cierto que en este caso se contemplan con mayor detalle:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la misma tenga por objeto el intercambio de datos de carácter médico entre facultativos o instituciones sanitarias y así lo exija el tratamiento del afectado, o la investigación epistemiológica de enfermedades o brotes epidémicos.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

Consideraciones Finales.

12. El movimiento internacional de datos está regulado de un modo autónomo en un capítulo específico de la Ley española de protección de datos. Al margen del relativamente escaso número de artículos referidos a este tema, esta autonomía es por sí misma significativa de la importancia otorgada por el legislador español a la cuestión. Por lo demás, aunque de forma tangencial, otros artículos de la LORTAD se refieren asimismo a la transmisión internacional de datos. Así, el artículo 36 que recoge entre las funciones de la Agencia de Protección de Datos el "ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos (...)", ó el artículo 43, que califica como infracción muy grave "la transferencia, temporal o definitiva, de datos de carácter personal (...) con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos".

13. El artículo 32 de la Ley establece la norma general en la materia: "no podrá realizarse transferencias (...) de datos de carácter personal (...) con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley".

En consecuencia, la posibilidad de tales transmisiones se hace depender de un criterio valorativo que si bien reside *prima facie* en el responsable del fichero, reposa de forma preeminente en la Agencia de Protección de Datos y, en concreto, en su Director. En efecto, en atención al propio artículo 32, cuando se obtenga autorización de este último, podrá formalizarse tal transmisión, aun cuando no se cumpla la condición general exigida.

El artículo 33, por otra parte, recoge toda una serie de excepciones que coinciden *grosso modo* con las excepciones enunciadas en los textos jurídicos internacionales sobre la materia.

14. En consecuencia, la ordenación de la transmisión internacional de los datos de carácter personal contenida en la LORTAD corre en buena medida en paralelo con la legislación internacional, circunstancia ésta que se aprecia tanto en las soluciones a las que se llega como en la técnica legislativa a la que se acude. Tal es el celo con el que el legislador español desarrolla esta labor de trasposición al derecho español de la normativa internacional que incluso incorpora a la LORTAD algunas de las deficiencias características del Derecho internacional de protección de datos, vg., la falta de rigor terminológica.

Bibliografía.

BLUME, P., "An EEC Policy for Data Protection", *Computer Law Journal*, vol. XI, nº 3, october 1992, pp. 399 y ss.

BRIAT, E, "Personal Data and the Free Flow of Information" en *Freedom of Data Flows and EEC Law. Proceedings of the 2nd. CELIM Conference*, Dordrecht: Kluwer, Computer Law Series, 1988, pp. 47 y ss.

GARZON, G, El marco jurídico del flujo de datos transfronteras, IBI Doc. TDF 102, Roma, 1981.

GARZON, G.; VILARIÑO, E, "Information and Privacy Protection in TDF? The Rights Involved", en OCDE, Transborder Data Flows and the Protection of Privacy, Paris: OCDE, 1979, pp 302 y ss.

HOWER, J.; DE BRABANT, K van, The TDF *of personal data. A comparative study of international and national regulation*, Bruxelles: Bruylant, 1989.

NUTGER, A.C.M. *TDF of Personal Data within the European Countries.*, Dordrecht: Kluwer, 1990.

PIÑOL, J.L.; "Los flujos internacionales de datos: aproximación a su regulación jurídica", *UNED*, Tomo IV Barbastro, 1987, pp. 135 y ss.

PIÑOL, J.L.; ESTADELLA, O., "La regulación sobre las transmisiones internacionales de datos en la LORTAD", en RIPOL, S. (Coord.), *La protección de los datos personales. Regulación nacional e internacional de la seguridad informática*, Barcelona: Centre d`Investigació de la Comunicació, 1993, pp. 75-92.

SAVAGE, R.N.; WALDENN, I.N., "Data Protection and Privacy Laws: Should Organizations Be Protected?", *ICLQ*, 1988, pp. 37 y ss.

SAUVANT, P., *International Transactions in Services: The politics of TDF*, New York: Westview Press, 1986.

SCHWEIZER, R.J., "La Convention du Conseil de l`Europe sur la protection des données personnelles et la régelementation des flux transfrontières de données", *Droit de l`informatique*, 1986/4 pp. 119 y ss.

La Agencia de Protección de Datos

MANUEL HEREDERO HIGUERAS
Subdirector de Cooperación Internacional del Ministerio de Justicia.

1. Introducción.

1.1. Todas las leyes de protección de datos que se han ido promulgando desde 1970 hasta 1992 han creado una autoridad especializada para su aplicación. Unicamente la *Privacy Act* norteamericana se abstuvo de crear una tal autoridad, encomendando a los tribunales ordinarios la solùción de los litigios que surgieran en la aplicación de la ley. Esta solución no es conciliable con el carácter preventivo del sistema protector de los datos que estas leyes configuran. La intervención de los órganos jurisdiccionales requiere que se haya producido el litigio y, por tanto, el daño o perjuicio imputable a la recogida y el uso indebido de los datos. Por otra parte, la aplicación del sistema protector, con el consiguiente registro de ficheros o equivalente, que haga posible el ejercicio del derecho de información, requiere una acción administrativa de gestión y una ordenación por vía reglamentaria. Esta es, sin duda, otra de las causas que hacían que la solución judicial no fuera idónea. Así se entendió en Francia, cuyo Código civil prohibe en su artículo 5 que los jueces y tribunales se pronuncien por vía de disposición general y reglamentaria en las causas a ellos sometidas; esto habría impedido el ejercicio de la potestad reglamentaria, que la ley francesa atribuiría a la Comisión Nacional de Informática y Liberta-

des (C.N.I.L.). Esta misma razón, de la necesidad de una acción conformadora, hace que la opción del Comisario parlamentario no sea tampoco suficiente por sí sola. Esto no implica que la autoridad especializada excluya toda actuación de los órganos jurisdiccionales ni tampoco del Parlamento. Todas las legislaciones prevén una revisión judicial de los actos de la autoridad especializada, así como algún tipo de control parlamentario que se encauza por la vía de una información anual o periódica en forma de memoria oficial.

1.2. Hasta la primera propuesta de Directiva comunitaria sobre protección de datos (SYN 287, 1990) no existe lo que podría denominarse una "teoría general" de la Autoridad especializada de protección de datos. El término de "Autoridad de control" no aparece hasta entonces como expresivo de un concepto genérico.

El Convenio 108 del Consejo de Europa soslayó esta cuestión. Su artículo 13 prevé un mecanismo de cooperación entre las Partes contratantes, pero, en realidad se trata de un mecanismo complementario del creado por otros Convenios del Consejo de Europa, como el Convenio 94, de Notificación en el Extranjero de Documentos Administrativos (1977) y el Convenio 100, de Obtención en el Extranjero de Informaciones y Pruebas en Materia Administrativa (1978). Se estimó que estos mecanismos no eran suficientes en el contexto de la protección de datos y, por otra parte, estos mismos convenios preveían la necesidad de completar el marco de cooperación que los mismos creaban, mediante acuerdos sobre ámbitos específicos. Por ello, el artículo 13 del Convenio 108 se limita a imponer a las Partes contratantes la obligación de designar una o varias autoridades, cuya denominación y ubicación deberán comunicar al Secretario General del Consejo de Europa. La Memoria Explicativa del Convenio (apartado 72) alude a la existencia de autoridades especializadas en protección de datos en la mayoría de los Estados, estimando por ello que no sería improbable que los Estados parte designaran precisamente a dichas autoridades especializadas como autoridades de enlace a los efectos del artículo 13. En todo caso, la Memoria (apartado 73) deja abierta la posibilidad de que las autoridades designadas sean otras. Tal ha sido el caso de Alemania Federal (Ministerios del Interior, federal y territoriales), o del Reino Unido (Secretaría del Interior). Fuera de este precepto, y con este limitado alcance, no se menciona la Autoridad de control de protección de datos, ni su creación se impone como obligación de las Partes, ni menos aún se da una pauta para su concepción.

1.3. La propuesta de Directiva comunitaria no podía limitarse a trasladar a su texto un modelo competencial que en el curso de cerca de una década y media se hubiera ido decantando en el plano doctrinal por vía de consenso. Si

bien existió siempre un acuerdo acerca de la necesidad de una tal autoridad y de la insuficiencia de la autoridad judicial; sin embargo, cada autoridad en concreto se basa en una concepción distinta. Ni aun puede decirse que sean órganos unitarios: en algunas legislaciones (Austria, Luxemburgo, Alemania, Reino Unido, Finlandia), la Autoridad de control consiste, en realidad, en un sistema o conjunto de órganos, que en la ley austríaca son, en realidad, tres. Por ello, resultaba imposible definir un modelo que pudiera albergar todas las variantes existentes. Cabría incluso definir una tipología, en función de la concepción del sistema protector que cada ley definía: un primer grupo vendría dado por las legislaciones escandinavas, orientadas a una acción de policía administrativa concretada en autorizaciones previas; un segundo grupo lo constituyen los órganos colegiados interpoderes (Francia, Portugal, Austria, Bélgica) o encuadrados en la Administración (Luxemburgo, Países Bajos).

1.4. La propuesta de Directiva SYN 287 - tanto la versión primitiva, de 1990, como la de 1992 - define un modelo a tal efecto en el artículo 30, completado por otros preceptos dispersos. Este modelo es fruto, a la vez, de un proceso de unificación y de una "extrapolación". La Comisión quiso incluir en la pauta estructural y competencial que define el precepto características que ya estaban presentes en todas las autoridades de control preexistentes. Pero asimismo añadió algunas características que, o bien estaban sólo apuntadas o definidas de manera imperfecta en la mayoría de las autoridades o sólo se daban en algunas de ellas. El resultado es que ninguna de las autoridades existentes se ajusta totalmente al modelo de la propuesta de Directiva: todas carecen de alguna o algunas de tales características. Por otra parte, las características del modelo no están claramente definidas y permiten una cierta variedad de opciones concretas.

1.5. La primera de las características que definen el modelo de la propuesta de Directiva es la de *independencia* (artículo 30-1). No se especifica en el precepto, ni tampoco en los "considerandos" del preámbulo lo que deba entenderse por "autoridad independiente". El "considerando" 29 se limita a repetir el término, pero sin añadir nada. La primera autoridad de control fue el Comisario de Protección de Datos del *land* de Hesse, creado por el § 8 de la ley de Protección de Datos de 1970. En este precepto aparece por primera vez el término "independencia". En el § 22 de la ley de dicho *land*, de 1986, que modificó la de 1970, figura asimismo esta exigencia como una de las notas definitorias del órgano. Con posterioridad, sólo aparece esta nota, de manera expresa, en el artículo 8, párrafo primero, de la ley francesa de 1978, en el § 2 de la ley noruega de 1978/1987, y en el artículo 4-2 de la ley portuguesa de 1991. Ninguna mención al respecto figura en las leyes de Dinamarca o Suecia. No existe, sin embargo, en la doctrina una noción de "administración

independiente" o de "ente independiente no administrativo". Cuando se aprobó la ley francesa, sólo existían en Francia dos órganos que pudieran ajustarse a este concepto (3), sin que hubiera una elaboración doctrinal.

1.6. El concepto de administración independiente puede ser entendido en varios planos: *designación* del titular o titulares; *exterioridad* a la estructura de la Administración del Estado; determinación del *contenido de los actos*; dotación de *medios* materiales, personales y financieros necesarios para el funcionamiento; *revisión* de los actos. Cabría admitir que es independiente una administración o ente público si el titular lo designa el Parlamento o el Jefe del Estado, no está inserto en la estructura de la Administración, los titulares no están sujetos a instrucciones en cuanto al contenido de los actos, el ente tiene medios propios, incluso patrimonio y presupuesto propios, y sus actos sólo son susceptibles de control de legalidad en sede jurisdiccional. Este modelo no lo cumple en su totalidad ninguna de las autoridades de control existentes, sin que tampoco pueda deducirse de ello que ninguna lo es. El elemento esencial que permite calificar un ente público de independiente es la no sujeción de sus actos a instrucciones de ningún otro órgano. Es el caso de las componentes de la C.N.I.L. (artículo 13, párrafo primero, de la ley). La Comisión austríaca es más explícita: el § 40 de la ley de 1978/1986 dispone que los componentes de la Comisión de Protección de Datos son "independientes y no están sujetos a instrucciones" (*an keine Weisungen gebunden*). Análogamente, el Comisario del *land* de Hesse. Cualquiera de los otros aspectos de la noción de independencia resulta problemático. El hecho de que la autoridad de control sea designada por el Parlamento (caso de las legislaciones de Alemania, Portugal o Finlandia) o por el Gobierno o por un Ministro o por el Jefe del Estado, es irrelevante. La designación parlamentaria, en sí misma, puede acarrear un riesgo de politización, en la medida en que la elección del titular o titulares pueda estar mediatizada por la correlación de las fuerzas políticas.

1.7. La independencia se refleja asimismo en la ausencia de un control jerárquico, en la "exterioridad" de la autoridad de control con respecto a la estructura de la Administración del Estado. Esta nota va íntimamente ligada a la no sujeción a instrucciones. Sólo cabe un control de legalidad por parte de los órganos de la jurisdicción. Algunas legislaciones lo prevén así expresamente, como la ley danesa de ficheros públicos (§ 21, párrafo quinto), según la cual las resoluciones de la Inspección de Ficheros no son recurribles ante ninguna otra autoridad administrativa. Asimismo, la Cámara de Registro de los Países Bajos. La (C.N.I.L.) sólo está sujeta al control del Tribunal de Cuentas. Las resoluciones de la Comisión austríaca sólo son revisables en vía contencioso-administrativa a nivel federal.

1.8. La propuesta de Directiva no limita a una sola la autoridad de control. El artículo 30-1, último inciso, permite que cada Estado designe varias autoridades de control. Cabe entender esta norma en varios sentidos. En primer lugar, puede referirse a determinadas autoridades de control que están compuestas de varias, como es el caso de Luxemburgo, que, en realidad, consta de un Ministro y de una Comisión Consultiva; o el del Reino Unido, cuya autoridad consta de un Registrador de Protección de Datos y de un Tribunal Administrativo. En la legislación alemana existen, a escala federal, el Comisario Federal de Protección de Datos y una autoridad administrativa de tutela, correspondiendo a uno y otra una competencia diversificada en función de la titularidad de los ficheros objeto del control. Otro aspecto de esta pluralidad de autoridades es el que hace referencia a la implantación territorial, pudiendo haber autoridades de control por cada Estado federado, Comunidad Autónoma, Región Autónoma, etc. Por último, cabe una pluralidad de autoridades por razón de la materia. A este respecto, cabe mencionar la Recomendación R (87) 15 del Consejo de Europa, sobre uso de datos con fines policiales, que prevé una autoridad independiente específica para el control de dicho uso. Por el momento, la ley de Luxemburgo parece hacer uso de esta posibilidad, en la medida en que el uso de los datos automatizados policiales lo ha colocado bajo el control directo del Ministerio Público en determinados aspectos (artículo 12-1).

1.9. El modelo de la propuesta de Directiva comprende unas funciones determinadas. El artículo 30-1 atribuye a la autoridad de control una función genérica de "ejercer el control de la protección de los datos personales". Esta función viene acotada por el propio precepto. No se trata de ejercer el control de la protección de los datos personales ilimitadamente, sino que debe contraerse a la vigilancia de la aplicación de las disposiciones nacionales adoptadas en aplicación de la Directiva. A este respecto, el artículo 3-2, primer guión, de la propuesta, dispone que el control de la protección de los datos personales objeto de tratamientos que no entren en el ámbito de aplicación del Derecho comunitario no será competencia de la autoridad de control. Esta exclusión se refiere principalmente a los ficheros y tratamientos policiales. Sin embargo, una vez que el Tratado de la Unión Europea vaya siendo ejecutado, estos ficheros y tratamientos estarán cubiertos por el Derecho comunitario y, por tanto, por la Directiva. Por otra parte, el primer "paquete" de actos incluidos en el primer proyecto de Directiva (1990) incluía un proyecto de resolución por el que los Estados miembros se comprometían a hacer extensiva la aplicación de la Directiva incluso a sectores no comprendidos en el ámbito del Derecho comunitario. Por ello no es fácil, por el momento, determinar el alcance exacto del ámbito de la Directiva. En todo caso, habrá que entender que esta obligación es un mínimo y que no es obstáculo a que

cada autoridad nacional de control extienda dicho control a ámbitos no cubiertos por la Directiva.

1.10. El modelo de la propuesta de Directiva se define, además, por unas potestades administrativas, mediante las cuales se ejerce la función genérica a que alude el artículo 30-1: potestad de *investigación* y potestad de *intervención*. Estas potestades se definen en el artículo 30-2. La primera consiste en acceder a los datos que sean objeto de los tratamientos y recabar toda información necesaria para el ejercicio de la función de control. La potestad de intervención consiste en ordenar el bloqueo o la supresión de datos, la prohibición provisional o definitiva de tratamientos, la destrucción de soportes de datos o la formulación de advertencias o apercibimientos a los responsables de los tratamientos. El artículo 30-2 añade a estas dos potestades la de *denuncia* a la autoridad judicial cuando haya comprobado la existencia de infracciones a las disposiciones nacionales adoptadas en aplicación de la Directiva. Esta norma sigue de cerca el modelo de la C.N.I.L. (artículo 21, párrafo primero, ap. 4° de la ley). En las legislaciones que atribuyen potestad sancionadora a su autoridad de control, esta función deberá entenderse como una función complementaria.

1.11. A las potestades del artículo 30-2 añaden los artículos 30-3 y 30-4 otras funciones, como la de sustanciar reclamaciones y denuncias, la de cooperar con las demás autoridades de control en la medida necesaria para cumplir su misión de control, y la de redactar una memoria anual de actividades que deberá ser publicada. No dice, sin embargo, si la memoria sólo se publicará o si deberá ser elevada oficialmente a algún órgano constitucional.

1.12. Las potestades y funciones del artículo 30 se completan con otras que se definen en preceptos diversos a las cuales se remite el propio artículo 30-1, cuando dispone que la autoridad de control independiente "ejercerá todas las funciones que la Directiva le asigna". Tales funciones se definen en los artículos 8-3, 12-3, 14-2, 19-2, 21 y 28-2. Los cuatro primeros atribuyen a la autoridad de control una habilitación para la *derogación singular* de algunos de los preceptos básicos de la Directiva. En primer lugar (artículo 8-3) en lo que respecta al tratamiento de datos sensibles, que el artículo 8-1 prohibe como norma general; asimismo, en cuanto a la obligación de informar al afectado en caso de comunicación de sus datos a un tercero, cuando el consentimiento para el tratamiento no sea preceptivo, o cuando sea imposible informarle o cuando ello implique esfuerzos desproporcionados o se oponga a los intereses legítimos del responsable del tratamiento o de un tercero (artículo 12-3). La autoridad de control puede igualmente exceptuar del derecho de acceso un determinado tratamiento, a petición del afectado, para lo cual debe proceder a las averiguaciones necesarias (artículo 14-2). Otras derogaciones singulares

que según la Directiva puede hacer la autoridad de control se refieren a la obligación de notificar los tratamientos, impuesta como norma general por el artículo 18: el artículo 19-2 faculta a la autoridad de control para exceptuar de la obligación de notificar o para prever una notificación simplificada.

1.13. Los artículos 18-4, 18-5, 21 y 28-2 definen una potestad que no se halla comprendida en la enumeración del artículo 30. Estos preceptos prevén una función de autorización previa, en la línea de las leyes danesas de ficheros privados y públicos, para los tratamientos que implicaren riesgos especiales para los derechos y libertades de las personas (artículos 18-4 y 18-5). Asimismo, la autoridad de control deberá comprobar la procedencia y representatividad de los códigos de conducta (artículo 28-2). El artículo 21 dispone, por último, que la autoridad de control lleve el registro de los tratamientos notificados, lo cual implica la atribución de una función certificante al respecto. En cambio, la propuesta de Directiva no atribuye a la autoridad de control competencia alguna en lo que respecta a la autorización de transferir datos a terceros Estados cuyo nivel de protección no sea el adecuado: el artículo 26 faculta en tal caso a los Estados miembros a que condicionen la transferencia de los datos a determinados supuestos.

1.14. La existencia de una autoridad de control especializada no implica la exclusión de la competencia propia de los órganos jurisdiccionales. La propuesta de Directiva reconoce expresamente dicha competencia en el artículo 22.

2. La Agencia de Protección de Datos como autoridad de control independiente.

2.1. El artículo 34-1 de la L.O. 5/1992, de 29 de octubre, creó la Agencia de Protección de Datos y el Real Decreto 428/1993, de 26 de marzo, la dotó de un Estatuto, cumpliendo lo dispuesto en el artículo 34-2, segundo inciso, y en la disposición final primera, de la L.O. 5/1993. El Estatuto de la Agencia no es la única disposición reglamentaria de desarrollo que la Ley prevé. Varios preceptos contienen habilitaciones reglamentarias específicas: así, los artículos 4-5 (procedimiento para la conservación de los datos de interés histórico), 9 (seguridad de los ficheros), 15-1 (plazo para hacer efectivo el derecho de rectificación o cancelación), 16-1 (procedimiento para ejercitar el derecho de acceso), 17-1 (reclamaciones por actos contrarios a la Ley), 24 (notificación de ficheros), 38-3 (procedimiento de inscripción de ficheros en el Registro General de Protección de Datos), sin perjuicio de la habilitación genérica de la disposición final primera. Siguiendo el criterio del Consejo de Estado, expresado en el dic-

tamen referente al proyecto de Estatuto (dictamen 97/93), se ha optado por un texto limitado a la estructura orgánica y funcional de la Agencia y a su régimen jurídico, económico, presupuestario y de personal, dejando para un momento posterior el resto del desarrollo reglamentario, debido a que, según el artículo 36 h) de la Ley, la Agencia debe informar preceptivamente los proyectos de disposiciones generales que desarrollen la Ley. El Consejo de Estado consideró, por ello, acertado regular primero el Estatuto de la Agencia y sólo una vez constituida ésta y nombrado el Director, ejercer la habilitación reglamentaria contenida en los demás preceptos de la Ley.

2.2. La Ley ha optado por crear un órgano especializado de control de su aplicación. A tal efecto, la ley define una solución original, adecuada al contexto jurídico-administrativo español. Con ello no ha hecho otra cosa que "repensar" el concepto a la luz del Derecho español, al modo de las demás leyes, como la ley del Reino Unido de 1984, que ha transpuesto a este contexto la fórmula usual del Derecho administrativo inglés, del Comisario real (Registrador) más un "tribunal administrativo", o las leyes escandinavas, que han utilizado la fórmula usual en sus Administraciones, del ente especializado regido por un Director que actúa bajo las directrices de un órgano colegiado que es parte del ente, a modo de Consejo de Administración. Las demás soluciones que ofrece el Derecho comparado obedecen a este mismo criterio o se deben a razones coyunturales.

Durante la tramitación parlamentaria, uno de los aspectos más controvertidos del proyecto fue precisamente éste de la concepción de la Autoridad de protección de datos y, en su caso, el de su inserción en el cuadro de los Poderes del Estado. Dos fueron, en términos generales, las posturas sustentadas por los Grupos parlamentarios que cuestionaron este aspecto del proyecto: a) Comisionado especial de las Cortes Generales, al modo del Defensor del Pueblo - pero sin limitar su acción a las quejas contra las Administraciones, sino haciéndola extensiva a la gestión de los ficheros privados - y b) órgano colegiado interpoderes. Se estimaba que, debido a la incidencia de la Ley en la esfera de los derechos y libertades individuales - "derecho de autodeterminación" sobre la información personal y consiguiente prohibición del acopio de datos sobre las personas sin el consentimiento de éstas -, sólo tales opciones eran válidas. Debía, por tanto, proscribirse toda intervención del Gobierno, del Ejecutivo, en la designación del órgano y en su funcionamiento. La realidad es que, a la vista de los diarios de sesiones de las Cámaras y de las escasas manifestaciones de opinión reflejadas en los medios de comunicación, ninguna de estas dos opciones estuvo defendida de manera convincente, sin que tampoco quepa excluir cierto mimetismo con respecto a algunas opciones del Derecho comparado - concretamente, el modelo francés de la C.N.I.L. La configuración

final de la Agencia, con el Consejo Consultivo como "colegio electoral" del Director, es fruto de una transacción en tal sentido. En el proyecto del Gobierno sólo figuraba el Consejo como un mero órgano de asesoramiento del Director. El modelo de la C.N.I.L. no es transplantable, pues se basa en una situación, hoy superada, en la que los ficheros más importantes y voluminosos eran los ficheros públicos, lo cual explica, entre otras cosas, su concepción como un órgano de mediación entre los Poderes públicos, así como su composición y el procedimiento de designación. Sólo la Comisión portuguesa (artículos 4 a 10 de la ley de 1991) ha seguido esta pauta. En rigor, pocos son los derechos y libertades que reconoce la Constitución, cuya vigilancia esté atribuida a órganos concebidos en tales términos. Normalmente son los órganos jurisdiccionales los que ejercen tal función, a tenor de lo previsto en el artículo 53 de la constitución. En el caso de la protección de la libertad religiosa, de los derechos de los consumidores y usuarios se ha optado por unos órganos de composición representativa de los interesados. Dentro de esta línea, habría sido más adecuado propugnar un órgano representativo que defendiera el derecho de autodeterminación de los titulares de datos, de los "afectados", por usar la expresión de la Ley.

2.3. La Ley ha creado un Ente público encuadrado en el género definido por el artículo 6-5 de la Ley General Presupuestaria (T.R. aprobado por R.D.L. 1091/1988). En este concepto se encuadran una treintena de entes y organismos de naturaleza heterogénea, tales como la Fábrica Nacional de Moneda y Timbre, la Comisión Nacional del Mercado de Valores, ENATCAR, RETEVISION, y, entre los más recientes, la Agencia Estatal de Administración Tributaria (1990), Puertos del Estado (1991) y Aeropuertos Españoles y Navegación Aérea (1990). La mayoría son entes prestadores de servicios, pero cabe diferenciar un subgrupo de entes, entre los que pueden encuadrarse, por ejemplo, la Agencia Estatal de Administración Tributaria o la Comisión Nacional del Mercado de Valores, cuyo fin es una función de control, no de prestación. Mediante el recurso a esta opción orgánica se aspira a lograr objetivos diversos, principalmente una mayor agilidad en la gestión de unos fines determinados, gracias a una derogación parcial de las leyes administrativas generales. En el caso de la Agencia de Protección de Datos, no ha sido tanto el deseo de una gestión ágil, como la necesidad de una independencia orgánica y funcional con respecto a los Poderes del Estado, lo que ha aconsejado esta opción.

2.4. La Agencia de Protección de Datos se ajusta al modelo definido en el artículo 30 de la propuesta de Directiva. La nota de *independencia* se recoge en el artículo 34-2 de la ley: la Agencia "actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones". Asimismo, según el artículo 16-2 del Estatuto, el Director "no estará sujeto a mandato imperati-

vo ni recibirá instrucciones de autoridad alguna". La designación del Director y del Consejo Consultivo corresponde al Gobierno, según el artículo 19-3 del Estatuto. La propuesta de nombramiento la eleva al Gobierno el Ministro de Justicia (artículo 19-2 del Estatuto). Tanto el Director como los vocales del Consejo Consultivo son inamovibles: el Director permanece en el cargo por un plazo de cuatro años a contar de su nombramiento (artículo 15-1 del Estatuto). Los vocales son asimismo nombrados por cuatro años (artículo 20-1 del Estatuto), excepto en el caso de que uno de ellos sea nombrado Director o en casos de renuncia o pérdida de la condición habilitante de su nombramiento (artículo 20-2 del Estatuto). El Director sólo cesa por acuerdo del Gobierno, pero sólo si se dan unas causas previstas taxativamente en la ley y en el Estatuto: expiración del plazo de mandato, renuncia, incumplimiento grave de sus obligaciones, incapacidad sobrevenida, incompatibilidad y condena por delito doloso (artículo 15-2 del Estatuto). El Director está sujeto a las incompatibilidades propias de los altos cargos (artículo 35-4 de la ley y 17 del Estatuto).

2.5. La Agencia y el Director no están sujetos a modalidad alguna de tutela administrativa. Sólo existe un *control de legalidad* de los actos del Director. Este control tiene su cauce en el recurso contencioso-administrativo previsto en los artículos 34-3 y 17-2 de la Ley, y en el artículo 2-4 del Estatuto. La Agencia, en el ejercicio de sus funciones públicas - es decir, no en la vertiente interna de gestión de su patrimonio, contratación, etc. - está sujeta a la legislación de procedimiento administrativo (actualmente, la ley 30/1992, de 26 de noviembre), y, en consecuencia, sus actos son recurribles directamente en vía contencioso-administrativa, ya que los actos del Director ponen fin a la vía administrativa (artículo 2-4 del Estatuto).

2.6. La ausencia de tutela administrativa es compatible con la existencia de unos cauces de *relación* con los Poderes del Estado. El Estatuto prevé tres cauces: a) relación entre la Agencia y el Gobierno, por conducto del Ministro de Justicia (artículo 1-2 del Estatuto); b) relaciones con las Cortes Generales, en la forma de traslado de la Memoria Anual de la Agencia a las Cortes Generales por el Ministro de Justicia (artículo 8-2 del Estatuto); c) relaciones con el Tribunal de Cuentas, por conducto de la Intervención General de la Administración del Estado (artículo 33-1 del Estatuto). El Ministro de Justicia sirve asimismo de cauce de relación con el Gobierno para la elección de los vocales del Consejo Consultivo, en la medida en que el artículo 19-2 del Estatuto le atribuye la función de proponer al Gobierno los nombres de los vocales. El Ministro de Justicia sólo determina la composición del Consejo mediante la propuesta del vocal que en el mismo deba representar a la Administración General del Estado; asimismo, en los supuestos de los vocales representantes de los consumidores y usuarios y de los titulares de los ficheros privados el Ministro de Justi-

cia debe elegir el vocal entre una terna propuesta respectivamente por el Consejo Nacional de Consumidores y Usuarios y por el Consejo Superior de Cámaras de Comercio. En los demás casos, el Ministro de Justicia se limita a trasladar al Gobierno las propuestas de las demás organizaciones representadas en el Consejo.

2.7. La *exterioridad* de la Agencia de Protección de Datos con respecto a la estructura de la Administración, como un aspecto más de la nota de independencia, se refleja en la ausencia del control de fiscalización de la Intervención General de la Administración del Estado. La Agencia no está tampoco sujeta al procedimiento de la fiscalización previa. El artículo 33-3 del Estatuto regula el control financiero en la forma del *control permanente*, incompatible con la fiscalización previa, y que está regulado por disposiciones específicas de la Intervención General de la Administración del Estado. Este control permanente no exime a la Agencia del control del Tribunal de Cuentas (artículo 33-1 del Estatuto), que, a su vez, no constituye una tutela, sino un control de otra naturaleza. La Intervención General de la Administración del Estado sólo sirve de cauce de relación entre la Agencia y el Tribunal (artículo 33-1 del Estatuto).

3. Estructura Orgánica de la Agencia.

3.1. El artículo 11 del Estatuto enumera como órganos de la Agencia los siguientes: a) el Director, b) el Consejo Consultivo, c) el Registro General de Protección de Datos, d) la Inspección de Datos, y e) la Secretaría General. Estos tres últimos tienen rango de Subdirección General (artículo 37-2 del Estatuto). Cabría añadir a estos órganos, a tenor de lo previsto en el artículo 30 del Estatuto, la secretaría del Consejo Consultivo, vinculada a la Secretaría General, y que el apartado c) de dicho artículo define como una función propia de la Secretaría General. Dentro del marco de la legalidad actual, el Estatuto no podía ir más allá de esta subdivisión del artículo 11, ya que, por debajo del nivel orgánico de Subdirección General no existen propiamente órganos, sino grupos de puestos de trabajo, a tenor de la reglamentación que se ha ido definiendo a partir de la ley 30/1984. El artículo 37 determina el régimen específico de las relaciones de puestos de trabajo de la Agencia, atribuyendo al Director una potestad de organización en el nivel de propuesta y referida a los puestos de trabajo en cuanto unidades orgánicas inferiores. La relación de puestos de trabajo la propone el Director a los órganos competentes por conducto del Ministro de Justicia (artículo 13-1 f), en relación con el 37-1, ambos del Estatuto). En cuanto a las relaciones entre la Agencia y los distintos órganos constitucionales, se hace remisión al organigrama adjunto y a lo expuesto en 2.5., *supra*.

3.2. Las funciones de los distintos órganos de la Agencia se definen en los artículos 12 a 31 del Estatuto. Los artículos 12 y 13 enumeran las funciones del Director, en su doble dimensión de órgano de decisión institucional (artículo 12) y de *manager* de la Agencia (artículo 13). El rango jerárquico y remuneración del Director son los propios de un Subsecretario (artículos 14-2 y 17). Los artículos 2-3, 2-4 y 12 del Estatuto han resuelto las ambigüedades que el texto de la ley ofrece en cuanto a una posible distribución de funciones entre el Director y la Agencia, en la medida en que la ley atribuye las funciones unas veces al Director y otras a la Agencia. Según el artículo 2-3, "la Agencia ejercerá sus funciones por medio del Director, a cuyo efecto los actos del Director se consideran actos de la Agencia". El artículo 2-4 completa esta norma, precisando que "los actos dictados por el Director en el ejercicio de las funciones públicas de la Agencia agotan la vía administrativa". La función de órgano de decisión institucional (*funciones de dirección*) que el artículo 2-3 le atribuye, se precisa en el artículo 12-2, según el cual corresponde al Director "dictar las resoluciones e instrucciones que requiera el ejercicio de las funciones de la Agencia". El citado precepto contiene a este efecto una enumeración *ad exemplum* de las funciones, que, por ello, son actos del Director y actos de la Agencia. Puede decirse, por ello, que *la Agencia es el Director*.

3.3. La dimensión de *manager* es la que define en términos generales el artículo 12-1 del Estatuto: el Director "dirige la Agencia y ostenta su representación". Esta función se desarrolla en el artículo 13 (*funciones de gestión*) y comprende la adopción de decisiones internas de la Agencia: contratación, ordenación de gastos y pagos, control económico-financiero, programación, presupuestos, relaciones de puestos de trabajo, convocatoria de las sesiones del Consejo Consultivo. Son las funciones que, a diferencia de las del artículo 12, no constituyen "funciones públicas de la Agencia" (artículo 2-4 *a contrario*). Si las primeras han de seguir el cauce de la legislación de procedimiento administrativo, las segundas se rigen por las disposiciones del Capítulo IV del Estatuto, que, en general, se remiten a la legislación presupuestaria y, por lo que respecta a las adquisiciones y contratos y régimen patrimonial, al Derecho privado.

3.4. El Director está asesorado por un *Consejo Consultivo* de composición representativa, regulado por el artículo 37 de la ley y por los artículos 18 a 22 del Estatuto en lo que respecta al procedimiento de propuesta y designación de sus vocales. La función asesora sólo la ejerce a instancia del Director, sin perjuicio de que formule propuestas sobre temas propios de la competencia de la Agencia (artículo 18). Además de esta función, le corresponde la de constituir el colectivo de candidatos a Director, ya que, a tenor de lo dispuesto en el artículo 14-2 del Estatuto, sólo los vocales del Consejo Consultivo pueden ser

propuestos por el Ministro de Justicia al Gobierno para su nombramiento como Director. Por último, corresponde al Consejo Consultivo la función de audiencia preceptiva en caso de separación del cargo en los supuestos previstos en el artículo 15-2: la separación se acuerda por Real Decreto, a propuesta del Ministro de Justicia, "oídos los restantes miembros del Consejo Consultivo". El Director, una vez nombrado, continúa siendo miembro del Consejo Consultivo, pero con el cargo de presidente (artículo 22-3).

3.5. Los demás órganos que enumera el artículo 11 del Estatuto son el Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General. Los dos primeros son los órganos de *line management*, en la medida en que ejercen, en el nivel funcional pertinente, las funciones anejas al fin institucional de la Agencia. La decisión corresponde al Director (artículo 14 del Estatuto), las funciones de propuesta de resolución e instrucción, en su ámbito respectivo, corresponden a estos dos órganos, a tenor de lo previsto en los artículos 23 y 26 (Registro General de Protección de Datos) y 27 a 29 (Inspección de Datos), asimismo del Estatuto. El tercero de estos órganos, la Secretaría General, tiene atribuida la función de apoyo logístico, ya que el apoyo operativo corresponde al Consejo Consultivo. Así resulta del artículo 30 del Estatuto. Dentro de esta función de apoyo logístico se encuadra el ejercicio de la función de secretaría del Consejo Consultivo (artículo 30 c) del Estatuto. La Secretaría General. La Secretaría General es también un órgano de documentación (artículo 31, a), b) c) del Estatuto). Por último, le corresponde una función de portavoz y de "jefe de relaciones públicas" de la Agencia, según el artículo 31 d), en relación con el 4-1, ambos del Estatuto: es la Secretaría General la que debe informar a las personas sobre los derechos que la ley les reconoce en el contexto de la protección de los datos personales, y a tal efecto promover campañas de difusión con ayuda de los medios de comunicación social.

4. Funciones de la Agencia.

4.1. Por lo que respecta a las funciones de la Agencia, se definen en la ley, en los artículos 36, 39, 48 y otros. El Estatuto se ha limitado a sistematizar y aclarar las que el artículo 36 de la Ley le atribuye. Todas las funciones definidas en el artículo 36 están presentes en el Estatuto. Las funciones de la Agencia se ajustan en general al modelo de la propuesta de Directiva comunitaria de protección de datos. La función genérica de control de la protección de datos la recoge el artículo 36 a) de la ley, según el cual es función de la Agencia "velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos". Esta función no se limita, sin

embargo, al control de la aplicación de la propia ley, puesto que el apartado m) del mismo artículo 36 le atribuye la función de velar asimismo por el cumplimiento de las disposiciones de protección de datos de la ley de la Función Estadística Pública. Esta función se concreta en el artículo 6 del Estatuto, que precisa que la Agencia ejerce el control de lo dispuesto en los artículos 4, 7, y 10 a 22 de la expresada ley. Para ello ejerce una función consultiva en relación con la confección de las hojas censales, cuestionarios y otros documentos de recogida de datos estadísticos, los procedimientos de recogida y proceso de los datos estadísticos, y las condiciones de seguridad de los ficheros creados con fines estadísticos.

4.2. La potestad de *intervención* a que se refiere el artículo 30-2 de la propuesta de Directiva se recoge en varios de los apartados del artículo 36 de la ley. En primer lugar, el apartado f): "ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de ficheros" cuando no se ajusten a las disposiciones de la ley. El artículo 48 de la ley atribuye a la Agencia una potestad de inmovilización de los ficheros. Se trata de una potestad complementaria de la potestad sancionadora que le atribuye el apartado g) del citado artículo 36 de la ley. El ejercicio de esta potestad de inmovilización es el último remedio de una cascada de medidas coercitivas que prevé la ley para los supuestos de infracción muy grave consistentes en la utilización o cesión ilícita de los datos que "impida gravemente" o "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. En estos casos, la Agencia incoará expediente sancionador y además podrá requerir al responsable del fichero a que cese en la utilización o cesión ilícita. Si el requerimiento fuera desatendido, la Agencia puede, por resolución motivada, ordenar la inmovilización del fichero, pero sólo a los efectos de restaurar los derechos de las personas afectadas. Esta cascada de medidas procede con relación a cualesquiera ficheros, públicos o privados. La diferencia estriba en que en el caso de los ficheros públicos, el expediente sancionador queda, en realidad sustituido por el expediente disciplinario contra los funcionarios adscritos al órgano responsable del fichero. El expediente sancionador carece de sentido entre órganos de la Administración, puesto que el resultado en caso de sanción no sería otro que una mera transferencia de crédito del órgano responsable al Tesoro en concepto de multa. Sin embargo, para que entren en juego el requerimiento y la inmovilización será preciso que el reglamento disciplinario incluya un supuesto análogo. Al margen de estas medidas del artículo 48, el artículo 45 prevé unas medidas coercitivas específicas para los casos en que las infracciones tipificadas en el artículo 43 sean cometidas en ficheros de las Administraciones públicas. En este supuesto, la Agencia puede, por resolución motivada, disponer las "medidas que proceda adoptar para que cesen o se corrijan los efectos

de la infracción", dando cuenta al responsable, a los afectados y al Defensor del Pueblo.

4.4. La potestad de *investigación*, que define el artículo 30-2 de la propuesta de Directiva, se recoge en el artículo 36 i) de la ley: "recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones", así como en el artículo 39, asimismo de la ley, y en el 28 del Estatuto. Según el artículo 39 de la ley, la Agencia puede inspeccionar los ficheros recabando cuantas informaciones precise para el cumplimiento de sus cometidos. A tal efecto puede solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, e inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales en los que se encuentren instalados. El artículo 28 del Estatuto desarrolla esta función inspectora e impone al responsable del fichero la obligación de permitir el acceso a los locales en que se hallen los ficheros y los equipos informáticos, previa exhibición de la autorización extendida al efecto por el Director, sin más limitaciones que las normas sobre inviolabilidad del domicilio.

4.5. La potestad de *denuncia* a que hace referencia el artículo 30 de la propuesta de Directiva puede ejercerla la Agencia por una doble vía. En primer lugar, dentro del marco de un expediente sancionador incoado a tenor de lo previsto en el artículo 36 g), si de las actuaciones del expediente resulta que los hechos son constitutivos de delito. Cabe que los hechos revelen la comisión de delitos tipificados en el Código penal, no sólo de los tipificados como delitos cuyo objeto sean los datos personales, como es el caso del artículo 198-2 del proyecto de Código penal de 1992. Cabe que las infracciones tipificadas en el artículo 43 de la ley concurran con otros hechos, como medio para cometerlos. Por otra parte, la Agencia, en cuanto persona jurídica dotada de plena capacidad jurídica pública y privada (artículo 34-2 de la ley y 2-1 del Estatuto), puede ejercer acciones civiles y criminales, al amparo de lo previsto en el artículo 38 del Código civil, y, en consecuencia, ejercer la acción pública y denunciar los hechos al Ministerio fiscal o al órgano jurisdiccional competente.

4.6. La función de publicidad registral que el artículo 21 de la propuesta de Directiva atribuye a la autoridad de control tiene su correspondencia en el artículo 38 de la ley y en el artículo 7 del Estatuto. Esta es la función que la ley española ha instrumentado mediante el Registro Nacional de Protección de Datos.

4.7. El modelo competencial de la propuesta de Directiva comprende asimismo (artículos 18-4, 18-5, 26 y 28-2) una competencia de intervención admi-

nistrativa -que no hay que confundir con la potestad de intervención que define el artículo 30-2- en varios supuestos, algunos de los cuales tienen un equivalente asimismo en la regulación de la Agencia. El supuesto del artículo 18-4 de la Directiva, que prevé, al modo del Derecho escandinavo, una autorización previa para ficheros que ofrezcan riesgos especiales para los derechos y libertades, no tiene correspondencia en la ley española. La ley española no atribuye esta competencia a la Agencia. El único caso en que la ley atribuye a la Agencia la potestad de autorización previa es el de la transferencia de datos a Estados extranjeros cuya legislación no ofrezca un nivel de protección de datos comparable al de la propia ley. Unicamente el artículo 31-2 de la ley confiere a la Agencia una competencia afín en cuanto a los códigos deontológicos, en la medida en que puede denegar su inscripción en el Registro General de Protección de Datos, recogiendo así la norma del artículo 28 de la propuesta de Directiva. Otras funciones previstas en el modelo comunitario (artículo 30), como la memoria anual y la cooperación internacional, se recogen igualmente en los artículos 36 k) de la ley y 8-2 del Estatuto, y en los artículos 36 l) de la ley 9 y 10 del Estatuto, respectivamente.

4.8. De las demás funciones que la propuesta de Directiva atribuye a la autoridad de control no tienen correspondencia en la legislación española las que entrañan una facultad de *derogación singular* de normas de la propia Directiva, como son la autorización para el tratamiento de los datos sensibles (artículo 8-3), la información en caso de cesión de datos a terceros (artículo 12-3), las excepciones discrecionales al derecho de acceso (artículo 14-2) y las exenciones o simplificaciones de la notificación (artículo 19-2).

4.9. A su vez, algunas funciones de la Agencia desbordan el modelo comunitario, como es el caso de la cooperación al desarrollo normativo, que regulan el artículo 36 c) y la disposición final segunda de la ley, y el artículo 5 del Estatuto.

Bibliografía.

No existen trabajos especializados que traten de las distintas autoridades nacionales de control de protección de datos. Sólo en algunos manuales generales o comentarios de las leyes correspondientes se puede encontrar un análisis de la respectiva autoridad de control. Sobre esta base, cabe mencionar los títulos siguientes: LUCAS, A., *Droit de l'informatique*, París, P.U.F., Thémis, 1987, págs. 158-177; HUET, J., MAISL, H., *Droit de l'Informatique et des Télécommunications*, París, Litec, 1989, págs. 166-171; DOHR, W., POLLIRER, E.M., WEISS, H.-J., *Datenschutzgesetz in der ab 1. März 1988 geltenden Fassung*, Viena,

Manz, 1988, págs. 147-167; DJONNE, E., GRONN, T., HAFLI, T., *Personregisterloven med kommentarer*, Oslo, TANO, 1987, págs. 36-46; FREESE, J., GAVATIN, Ch., RYDEN, N., *Privatlivets helgd*, Estocolmo, LiberFörlag, 1975, págs. 47, 72, 102; *En ny datalag*, Statens offentliga utredningar 1993:10, Malmö 1993; NIBLETT, B., *Data Protection Act 1984*, Londres, Oyez Longmann, 1984, págs. 24-26 y 83; AUERNHAMMER, H., *Bundesdatenschutzgesetz*, Colonia, Heymanns, 2ª ed., 1981; ORDEMANN, H.-J., SCHOMERUS, R., GOLA, P., *Bundesdatenschutz mit Erläuterungen*, 5ª ed., Munich, C.H.Beck, 1992; *Het ontwerp van Wet persoonsregistratie*, Alphen a.d.Rijn, Samsom, H.D.T.Willink, 1985; *Botschaft zum Bundesgesetz über den Datenschutz* (mensaje del Consejo Federal suizo al Presidente Federal,de 23 de marzo de 1988, 88.032).

Textos.

Por lo que respecta a las fuentes normativas, hay que hacer remisión a los textos legales y reglamentarios correspondientes. Las leyes no siempre ofrecen el detalle suficiente y muchas se remiten a disposiciones reglamentarias de desarrollo. Los textos pertinentes son los que siguen. **Alemania**: ley federal de protección de datos, de 20 de diciembre de 1990, versión española publicada en el "B.I.M.J." núms. 1630 y 1631; **Austria**: ley federal de 18 de octubre de 1978, de protección de los datos personales, modificada por la ley de reforma de 27 de junio de 1986, ley 370/1986, versión española en el volumen "Leyes de Protección de Datos", Madrid, M.A.P., 1987; **Bélgica**: ley de 8 de diciembre de 1992, relativa a la protección de la vida privada con relación a los tratamientos de datos de carácter personal, "Moniteur Belge", 18 de marzo de 1993; **Dinamarca**: ley de ficheros privados, núm. 293, de 8 de junio de 1978, modificada por ley núm. 383, de 10 de junio de 1987; ley de ficheros de las autoridades públicas, núm. 294, de 8 de junio de 1978, modificada por la citada ley núm. 383, de 10 de junio de 1987, versión española de ambos textos en el volumen citado; véase asimismo la Orden de aplicación de la ley de 1987, Orden del Ministerio de Justicia núm. 621, de 2 de octubre de 1987 (Bekendtgorelse af lov om offentlige myndigheders registre); **Finlandia**: Personregisterlag, 30 de abril de 1987; lag om datasekretessnämnden och dataombudsmannen, 30 de abril 1987, "Finlands Författningssamling", 8 mayo 1987; **Francia**: ley núm. 78-17, de 6 de enero de 1978, relativa a la Informática, los Ficheros y las Libertades, versión española en el volumen citado; véase asimismo el Decreto núm. 78-774, de 17 de julio de 1978, de aplicación de los Capítulos I a IV y VII de la ley 78-17, "J.O." de 23 de julio de 1978; **Luxemburgo**: texto coordinado de 2 de octubre de la ley de 31 de marzo de 1979, de regulación de los datos nominativos en los tratamientos informáticos; **Noruega**: ley 48, de 9 de junio de 1978, modificada por la ley de reforma de 12 de junio de 1987, versión española en el

volumen citado; véase asimismo la Orden del Ministro de Justicia de 21 de diciembre de 1979, dictada en aplicación de la Resolución real de 21 de diciembre (Forskrift om personregistre m.m. og om delegasjon av myndighet); **Países Bajos**: Wet van 28 december 1988 houdende regels ter bescherming van de persoonlijke levensfeer in verband met persoonsregistraties "Statsblad" 665; **Portugal**: ley núm. 10/91, de protección de datos con respecto a la informática, "Diario da República", 29 de abril 1991; **Suecia**: ley 289/1973, modificada por última vez por la ley 446/1982, de 3 de junio de 1982, publicada en 21 de junio, versión española en el volumen citado; véase la Instruktion för datainspektionen (1988:912); **Suiza**: Bundesgesetz über den Datenschutz vom 19. Juni 1992.

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Comisario Federal de Protección de Datos (República Federal de Alemania).	Organo unipersonal.	Depende funcionalmente del Ministro Federal del Interior. En el ejercicio del cargo, es independiente y sólo está sujeto a la ley.	Elegido por la Dieta Federal, siempre que estén presentes más de la mitad del número legal de sus componentes, a propuesta del Gobierno Federal, de entre personas mayores de 35 años. Nombrado por el Presidente Federal. Plazo de mandato, cinco años. Puede ser reelegido una sola vez. Cesa por expiración del mandato, o a petición propia. El Presidente Federal puede destituirlo si se dan las causas que justifican el cese en un juez nombrado en propiedad.	Memoria bienal a elevar a la Dieta Federal. Evacua dictámenes e informes a instancia de la Dieta, la Comisión de Petición o la Comisión de Interior, o el Gobierno Federal. Eleva recomendaciones al Gobierno Federal	Control de la aplicación de la legislación federal de protección de datos. Denuncia de violaciones de la legislación federal de protección de datos por los organismos públicos federales. Llevanza de un registro de ficheros automatizados de datos personales gestionados por los organismos públicos federales.	Tutela de legalidad del Gobierno Federal.	Presupuesto de gastos del Ministerio Federal del Interior.

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Comisión de Protección de Datos (Austria).	Organo colegiado, de 4 mienbros con experiencia en materia de protección de datos, nombrados por cinco años y reelegibles: 1perteneciente a la carrera judicial. 2 designados por los länder. 1 a proponer de entre los funcionarios federales sabedores en Derecho. El miembro perteneciente a la carrera judicial ejerce la presidencia. Cada miembro tiene un suplente. Uno de los miembros asume la gestión diaria de los asuntos.	Los miembros son independientes en el ejercicio de su cargo y no están vinculados por instrucciones de ningún órgano.	El Presidente Federal, según propuesta del Gobierno Federal, hecha por el canciller Federal. El miembro de la carrera judicial lo elige el Canciller Federal de entre una terna formada por el Presidente del Tribunal Supremo. Cese por fallecimiento, dimisión o destitución por la Comisión en caso de faltar tres veces seguidas a las sesiones, sin justificación, o en caso de incompatibilidad sobrevenida, oída la Comisión.	La gestión administrativa corresponde al Canciller Federal. El Canciller Federal pone a su disposición el personal necesario. Informe bienal al Canciller Federal.	Resolver reclamaciones en caso de lesión de los derechos de los afectados. Intervenir como coadyuvante en procesos civiles fundados en incumplimiento de la ley de protección de datos. Requerir a los responsables de los ficheros a que subsanen omisiones e incumplimiento de las disposiciones de la ley. Resolver sobre las inscripciones en el Registro de Tratamientos de Datos. Autorizar las transferencias internacionales de datos. Dictar su reglamento interno	Revisión de los actos ante el Tribunal Federal Contencioso Administrativo.	Tasas de inscripción en el Registro de Tratamientos de Datos.

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Consejo de protección de Datos (Austria).	Organo colegiado representativo: 4 representantes del partido más representado en el Parlamento. 3 del que le siguiere en representación. 1 por cada otro partido. 1 representante de la Cámara Austríaca de Trabajadores. 2 representantes de los Estados. 1 representante de la Liga de Municipios. 1 representante de la Liga de Ciudades. 1 representante de la Federación.		Organos y corporaciones representados.	Memoria anual a elevar al Canciller Federal.	Organo de reflexión, observación y propuesta en materia de protección de datos.		
Registro de Tratamientos de Datos (Austria).	Organo regular.	Oficina Central Austríaca de Estadística. Sujeto a instrucciones del Canciller Federal.			Llevanza del registro público de tratamientos.		

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Comisión de la protección de la vida privada (Bélgica).	Organo colegiado de un número variable de miembros, en todo caso por partes iguales de expresión francesa y de expresión neerlandesa. a) Miembros de derecho representantes de comités de vigilancia creados por leyes especiales; su número no puede exceder de la mitad del total; un comité de vigilancia sólo puede estar representado por dos miembros. b) 8 miembros efectivos, entre ellos un juez, que asume la presidencia. c) 8 miembros suplentes, entre ellos un juez. Además del presidente, debe haber entre los miembros efectivos y entre los miembros suplentes asimismo, un jurista, un informático, una persona con experiencia en la gestión de ficheros privados de datos personales y otra con experiencia en la gestión de ficheros públicos de datos personales. La composición debe reflejar un equilibrio socioeconómico.	Comisión independiente adscrita al Ministerio de Justicia. El personal de la secretaría está adscrito al Ministerio de Justicia. Ni el presidente ni los miembros de la Comisión reciben instrucciones de nadie, ni pueden ser relevados en razón de opiniones vertidas o actos realizados en cumplimiento de su función. El presidente ejerce el cargo con plena dedicación.	Los miembros de derecho los nombran las Comisiones de vigilancia. Los miembros efectivos los nombran, por turno, la Cámara de Representantes y el Senado, con un mandato de seis años renovable, sobre la base de listas con un mínimo de dos candidatos por puesto, propuestas por el Consejo de Ministros. Los candidatos deben ofrecer garantías de independencia. Son destituidos por la Cámara que los nombra, en caso de faltar a sus deberes o atentar a la dignidad de su función.	Memoria anual a las Cámaras legislativas. Denuncia al Procurador del Rey las infracciones de que tenga conocimiento. El presidente somete al tribunal de primera instancia los litigios referentes a la aplicación de la ley de protección de datos y de sus medidas de ejecución.	Emitir, a instancia de los Comités de vigilancia, del Gobierno, de las Cámaras o de los órganos regionales, municipales o de las comunidades de población, dictámenes, y asimismo recomendaciones con destino a los responsables de los ficheros, en materias propias de la ley. Llevar un registro, accesible al público, de los tratamientos automatizados de datos personales, previa su notificación a la Comisión. Proponer o informar reales decretos de autorización de la interconexión de tratamientos de datos y la transferencia de datos al extranjero.		Gastos de la Comisión y de su secretaría, a cargo del Ministerio de Justicia. La notificación de los ficheros devenga una tasa, cuyo importe lo fija el Rey, sin que pueda exceder de 10.000 FB.

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Inspección de ficheros (Dinamarca).	Consejo, compuesto de un presidente y otros 6 miembros. Secretaría, dirigida por un director.	El Ministro de Justicia aprueba el reglamento de régimen interior del Consejo y la distribución de tareas entre el Consejo y la Secretaría. El Ministro de Justicia puede exceptuar de la obligación de autorización previa las transferencias internacionales de datos.	El Ministro de Justicia nombra al presidente, de entre personas que reúnan los requisitos de habilitación para ser nombrado juez. El Ministro de Justicia nombra a los otros seis miembros y a los suplentes. El mandato del presidente y de los miembros es de cuatro años.	Memoria anual, a elevar al Parlamento.	Velar, de oficio o a instancia de los afectados, por que los ficheros sean creados y llevados de conformidad con la legislación de protección de datos. Autorizar lacreación y llevanza de ficheros, en los casos previstos en la legislación. Requerir de los responsables de los ficheros, públicos y privados, la información precisa para ejercer sus funciones. Inspeccionar, previa autorización los locales en los que se llevan los ficheros. Formular advertencias a los responsables de los ficheros en caso de incumplimiento de la legislación, debiendo ser informada de las medidas que se adopten. Elevar propuestas de reforma de la legislación a las Autoridades dotadas de potestad reglamentaria. Autorizar transferencias internacionales de datos.	Contra las resoluciones referentes a los ficheros privados no procede recurso en vía administrativa.	Percepción de tasas por comunicar datos en virtud del ejercicio del derecho de acceso a los ficheros públicos. Percepción de tasas por notificaciones y autorizaciones.

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Defensor de los datos (Finlandia).	Organo unipersonal. Asistido por una secretaría, cuyo jefe es Defensor adjunto. El Defensor adjunto puede ejercer acciones por delegación del Defensor.	Adscrito al Ministerio de Justicia. Es incompatible con otro servicio del Estado u otra ocupación durante el tiempo que dure su mandato.	Es nombrado por el Presidente de la República, entre licenciados en Derecho, a propuesta del Consejo de Estado (Consejo de Ministros), por un período máximo de cinco años.	Memoria anual, a elevar al Ministro de Justicia.	Ordena la inspección de ficheros, pudiendo servirse de expertos nombrados por el Comité de Datos Secretos. En el ejercicio de la inspección puede acceder a los locales, datos y sistemas informáticos. Dicta instrucciones sobre recogida masiva de datos sensibles. Autoriza la interconexión de ficheros, en los casos en que no debe hacerlo el Comité de Datos Secretos. Vigila el cumplimiento de las obligaciones de los responsables de los ficheros en relación con los derechos de acceso y rectificación. Propone al Comité de Datos Secretos medidas para subsanar el incumplimiento de la legislación. Lleva un registro de notificaciones de ficheros. Sigue la evolución general en materia de protección de datos y asume la cooperación internacional en la materia.		Retribución según contrato. Dictámenes retribuidos según disponga el Ministerio de Justicia, oído el de Hacienda.

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Comité de Datos Secretos (Finlandia).	Organo colegiado, compuesto de: 1 presidente. 1 vicepresidente. 5 vocales. Cada miembro tiene un suplente.	Adscrito al Ministerio de Justicia.	Lo nombra el Consejo de Ministros (Consejo de Estado) por tres años. El presidente, el vicepresidente y un vocal y su suplente deben ser licenciados en Derecho.		Autoriza las transmisiones internacionales de datos. Puede prohibir o hacer cesar tratamientos de datos contrarios a la ley. Autoriza el registro de datos con fines de valoración de la solvencia y control de morosos. Autoriza el registro de datos sensibles.		

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Comisión Nacional de la Informática y las Libertades (Francia).	Organo Colegiado de 17 miembros (más el Delegado del Gobierno). 2 diputados. 2 senadores. 2 vocales del Consejo Económico y Social. 2 miembros o ex miembros del Consejo de Estado. 2 miembros o ex miembros de la Corte de Casación. 2 miembros o ex miembros del Tribunal de Cuentas. 2 expertos en informática nombrados por Decreto a propuesta de los presidentes de la Asamblea y del Senado. 3 personalidades nombradas por Decreto. Mandato de cinco años o del tiempo que dure el cargo habilitante. 1 Presidente y 2 vicepresidentes elegidos por 5 años por la Comisión.	Autoridad administrativa independiente. Sus miembros no reciben instrucciones de ninguna autoridad. La calidad de miembro es incompatible con la de miembro del Gobierno y con el ejercicio de cargos en empresas de fabricación o distribución de material informático.	Nombramiento por los órganos representados. Cese por expiración de mandato o dimisión.	Un delegado del Gobierno forma parte de la Comisión. La Comisión puede requerir a los presidentes de los tribunales de apelación o de lo contencioso administrativo a que deleguen a un juez para misiones de investigación y control. Informe anual al Parlamento.	Potestad reglamentaria. Informe previo a la creación de tratamientos de datos. Inspección. Apercibimientos a los responsables de los ficheros. Denuncia al Ministerio Público. Lista oficial de ficheros. Autorización de transferencias internacionales de datos.	Tribunal de Cuentas.	Presupuesto de gastos incluido en el del Ministerio de Justicia. Posibilidad de percibir tasas.

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Ministro encargado del Repertorio Nacional de Bancos de Datos (Ministro de Justicia) (Luxemburgo).		Gobierno.	Gran Duque.	Denunciar a la autoridad judicial las infracciones de la legislación de protección de datos.	- Velar por el cumplimiento de la legislación de protección de datos. - Autorizar la creación y la explotación de los bancos de datos no dependientes del Estado. - Inscribir los bancos de datos en el Repertorio Nacional. - Ordenar inspecciones, solicitar explicaciones, formular recomendaciones y librar requerimientos. - Resolver reclamaciones. Control del ejercicio de los derechos de los afectados.	Las resoluciones del Ministro, por las que se concede, deniega o revoca la autorización para crear y explotar un banco de datos son recurribles ante el Consejo de Estado, Comité de lo Contencioso, en el plazo de un mes a partir de la notificación de la resolución.	

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Comisión Consultiva (Luxemburgo).	Organo colegiado de cinco miembros.	Ministro encargado del Repertorio Nacional de Bancos de Datos. (Ministro de Justicia).	El Gran Duque nombra a los miembros, por un plazo de cinco años. Los miembros se eligen entre juristas e informáticos de los sectores público y privado. Mandato renovable.	Asesora e informa al Gobierno.	Emitir dictámenes. Asesorar al Gobierno. Denunciar al Gobierno abusos o deficiencias no previstos en la legislación de protección de datos. Memoria anual al Gobierno.		

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Inspección de Datos (Noruega).	Consejo de Dirección de 7 vocales. Administración, dirigida por un Director.	Organo administrativo ordinario, adscrito al Departamento de Justicia.	El Rey nombra a los vocales del Consejo de Dirección, por un plazo de cuatro años. El Rey nombra asimismo al presidente y al vicepresidente. Los vocales son nombrados *intuitu personae y no representan a sectores sociales u organizaciones.*	Memoria anual elevada al Ministro de Justicia, que la eleva al Parlamento.	Autorizar los ficheros automatizados de datos personales, en los casos previstos por la ley de protección de datos, y dictar normas para el uso de los ficheros autorizados. Informar proyectos de disposiciones que inciden en la protección de datos. Sustanciar quejas y evacuar los informes pertinentes o dictar normas de obligado cumplimiento, en su caso. Vigilar el cumplimiento de la legislación de protección de datos. Evacuar informes, de oficio o a instancia de parte, en materias que impliquen el uso de ficheros o de datos personales en general. Autorizar transferencias de datos y ficheros a países extranjeros. Promover campañas de difusión de la protección de datos.	Recurso en vía administrativa ante el Departamento de Justicia. El Ministro de Justicia puede reclamar contra los responsables de los ficheros que dependen del Departamento, en cuyo caso la reclamación la instruye el Departamento de Consumidores y Administración y resuelve el Rey.	Presupuesto propio.

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Cámara de Registro (Países Bajos).	Organo colegiado. 1 presidente. 2 miembros. Otros miembros, en número variable. Miembros suplentes. Miembros extraordinarios. Organos: - 1 vicepresidente primero. - 1 vicepresidente segundo. - Una Secretaría. - Una Sección Central, formada por el presidente y dos miembros.		El presidente es nombrado por Real Decreto, a propuesta del Ministro de Justicia, por un período de mandato de seis años y puede ser reelegido en todo momento. Los miembros, los miembros suplentes y los miembros extraordinarios son nombrados por Real Decreto, a propuesta del Ministro de Justicia, por un período de mandato de cuatro años, y sólo pueden ser reelegidos una vez. Los vicepresidentes primer y segundo son nombrados de entre los miembros de la Cámara por Real Decreto, a propuesta del Ministro de Justicia. Todos los miembros titulares, suplentes y extraordinarios, cesan al comenzar el primer mes subsiguiente a la fecha en que cumplen 65 años. El primero y segundo vicepresidentes son nombrados por Real Decreto a propuesta del Ministro de Justicia. El personal de la secretaría lo nombra y cesa el Ministro de Justicia.	Memoria anual, redactada por la Sección Central, a elevar al Ministro de Justicia.	Asesorar al Ministro de Justicia y, en su caso, a los demás Ministros, según su competencia, a su instancia o de oficio, sobre la aplicación de la legislación de protección de datos. Investigaciones, de oficio o a instancia de un afectado, sobre la adecuación de la llevanza de los ficheros a lo dispuesto en la legislación de protección de datos, dando cuenta de su resultado al afectado, si procede, o formulando recomendaciones al responsable del fichero. Proponer al Ministro de Justicia resoluciones sobre transferencias internacionales de datos. Los miembros y el personal tienen acceso a los locales en que se hallen los ficheros, sólo con autorización expresa de la Cámara.	Contra las resoluciones de la Cámara no procede recurso en vía administrativa.	

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Comisión Nacional de Protección de Datos Personales Informatizados (Portugal).	Organo colegiado de siete miembros. 1 presidente. 2 diputados. 1 juez con más de 10 años de ejercicio. 2 personalidades competentes en la materia. Servicios propios de apoyo técnico y administrativo.	Ente público independiente.	El presidente y los diputados los nombra la Asamblea por el método de la media más alta de d'Hondt. El juez lo nombra el Consejo Superior de la Magistratura. El fiscal lo nombra el Consejo Superior del Ministerio Público. Las dos personalidades con competencia en la materia las nombra el Gobierno. Mandato de cinco años, que se prorroga hasta la toma de posesión de los nuevos miembros.	Adscrita a la Asamblea. Se relaciona con la Asamblea y con la Autoridad Judicial y el Ministerio Público.	Dictaminar sobre la creación, modificación o conservación de ficheros, bases de datos y bancos de datos personales, de titularidad pública o privada. Autorizar en casos excepcionales el uso de los datos para fines no previstos en la recogida. Autorizar la interconexión de bases y bancos de datos. Dictar normas de seguridad. Id. sobre acceso, rectificación y actualización de datos. Resolver reclamaciones, quejas y peticiones. Autorizar transferencias internacionales de datos. Memoria anual. Proponer a la Asamblea medidas que convengan al ejercicio de sus atribuciones. Promover, de acuerdo con la autoridad judicial, medidas de intervención, inmovilización o destrucción de ficheros. Ejercitar la acción pública en casos de violación de la ley de protección de datos.	Reclamaciones y recursos ante el Supremo Tribunal Administrativo.	La remuneración de los miembros la fija el Gobierno.

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Registrador de Protección de Datos (Reino Unido).	Organo unipersonal. Asistido por un Vice-Registrador y personal adscrito.	No es funcionario o agente de la Corona, excepto a efectos de la ley de Secretos Oficiales. El Secretario del Interior nombra al personal adscrito al Registrador. El Secretario del Interior ejerce la potestad de interpretación y aplicación de la ley, previa audiencia del Registrador.	Nombramiento por la Reina, por Cartas Patentes, a propuesta del Primer Ministro, por cinco años. Cese por expiración del plazo de cinco años, por dimisión, por destitución acordada por la Reina en virtud de moción de las dos Cámaras del Parlamento y por transcurso del año en el cual cumpliere 65 años, pudiendo ser nombrado de nuevo si cesare por expiración del mandato.	Memoria anual a elevar a cada una de las Cámaras del Parlamento. Informes discrecionales a elevar a cada Cámara.	Decidir sobre la inscripción de los usuarios de datos y de los prestadores de servicios informáticos relativos a datos personales, sobre la modificación y cancelación de las inscripciones. Sustanciar quejas motivadas por incumplimiento de la ley. Fomentar la elaboración de códigos de conducta. Autoridad de cooperación a los efectos del Convenio 108 (art.13). Autorizar o prohibir la transferencia de datos a países extranjeros. Control financiero permanente, según las instrucciones del Secretario del Interior.	Recurso en vía administrativa ante el Tribunal Administrativo. Revisión judicial de las resoluciones del Tribunal Administrativo ante el Alto Tribunal de Justicia de Inglaterra y Gales, el Court of Session de Escocia o el Alto Tribunal de Justicia de Irlanda del Norte. Control contable a cargo del Interventor General.	Retribución y pensión acordadas por la Cámara de los Comunes. Tasas y otras cantidades devengadas por el ejercicio de sus funciones, a ingresar en el Fondo Consolidado.

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Tribunal Administrativo de Protección de Datos (Reino Unido).	Organo Colegiado compuesto por un presidente nombrado por el Lord Procurador de Escocia, varios vicepresidentes nombrados en igual forma, y varios vocales nombrados por el Secretario del Interior, de entre letrados y procuradores con siete años de ejercicio, en representación de los usuarios de datos y los prestadores de servicios informáticos.				Revisión en vía administrativa de los actos del Registrador.		

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Inspección de Datos (Suecia).	Consejo de dirección, de carácter representativo, formado por diez miembros. Uno de los miembros es el presidente. Para los otros nueve miembros hay cinco suplentes. El presidente del Consejo de dirección es jefe de la Inspección de Datos. Tres unidades orgánicas: autorizaciones, inspección y secretaría. Uno de los jefes de unidad es jefe adjunto de la Inspeción de Datos. Las resoluciones son colegiadas, excepto en casos determinados, en los que resuelven el jefe y el jefe de la unidad correspondiente, debiendo, en todo caso, dar cuenta en la reunión siguiente del consejo de dirección.	Ente independiente.	El Rey nombra a los miembros del Consejo y a los suplentes, por cuatro años. El Rey nombra al jefe de la Inspección por tiempo indefinido. El jefe de unidad que ejerce las funciones de jefe adjunto lo nombra el Rey por tres años a propuesta del jefe de la Inspección.	Sólo se relaciona con el Rey.	Autorizar la creación y explotación de ficheros de datos personales. Revocar autorizaciones. Dictar normas de explotación para los ficheros autorizados. Inspección de ficheros. Autorizar transferencias internacionales de datos. Vigilar el cumplimiento de la ley de Datos, de la ley de Información crediticia y de la ley de Cobros por Cuenta Ajena.	Recurso de alzada ante el Rey. El Canciller de Justicia está legitimado para interponer el recurso en defensa del interés general.	Autofinanciación mediante exacción de tasas por las autorizaciones.

Denominación	Estructura	Dependencia	Nombramiento y Cese	Relaciones con los Poderes del Estado	Funciones	Control de los actos	Financiación y Patrimonio
Comisario Federal de Protección de Datos (Suiza).	Organo unipersonal. Asistido de una Secretaría permanente.	Depende administrativamente del Departamento Federal de Justicia y Policía.	Consejo Federal.	Informes periódicos a elevar al Consejo Federal. Informes a elevar al Consejo Federal cuando fuere necesario.	- Controlar la aplicación de la ley federal de protección de datos. - Potestad de investigación. - Formular recomendaciones sobre el uso de los datos personales cuando de la investigación resulte que dicho uso es contrario a la ley. - Asistir a los particualares y a los órganos federales y cantones sobre el uso de los datos. - Informar preceptivamente los proyectos de disposiciones y medidas federales que incidan en la protección de datos. - Cooperar con las Autoridades internas y extranjeras de protección de datos. - Dictaminar sobre si la protección de datos en el extranjero es comparable con la Suiza. - Asesorar al comité de Expertos sobre el Secreto Profesional en relación con la investigación médica.	Recurso ante la Comisión Federal de Protección de Datos.	

Estatuto de la Agencia de Protección de Datos

(REAL DECRETO 428/1993)

CINTA CASTILLO JIMENEZ

Profesora de la Universidad de Sevilla.

El presente trabajo supone un análisis del contenido del Real Decreto 428/1993, de 26 de Marzo, por el que se aprueba el estatuto de la Agencia de Protección de Datos.

El título VI de la Ley Orgánica 5/1992, de 29 de Octubre, sobre la Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), configuró la Agencia de Protección de Datos como el ente independiente que debe garantizar el cumplimiento de las previsiones y mandatos en ella establecidos.

Algunos de los aspectos de este ente han sido regulados en la propia ley orgánica, pero la mayoría de ellos se dejaron encomendados desde la propia ley a un desarrollo normativo posterior.

Así por medio del Estatuto se procede a complementar el mandato hecho desde la propia ley orgánica, integrando la estructura de este ente en su propia norma.

El Real Decreto no ha entrado en vigor hasta el 24 de Mayo pasado, por lo que aún no se puede hablar del funcionamiento de la Agencia, nos ceñiremos por tanto, en nuestro análisis al texto de la norma, para estudiar como ha quedado configurada ésta.

La LORTAD, dedica el título VI a la Agencia de Protección de Datos, pero no agota su regulación, remitiéndose a un reglamento posterior, de forma amplia y generosa tanto en aspectos relativos a su estructura y funcionamiento interno, como en lo referente al ejercicio de sus atribuciones.

La Agencia se perfila desde la LORTAD, Art. 34 y Art. 1.2 de su Estatuto, como un ente que actuará con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones, relacionándose con el gobierno a través del Ministerio de Justicia. Respecto a esto, se han dado ciertas polémicas y numerosas críticas, fundadas la mayoría de ellas en la naturaleza eminentemente administrativa que la ley le ha adjudicado.

En el trámite legislativo, se hicieron algunas propuestas con la finalidad de configurar a la Agencia al modo de la Comisión Nacional de la Informática y las Libertades francesa, es decir como un órgano colegiado, en relación con las Cortes y no con el Gobierno como queda regulado en su Estatuto.

Así la institución podrá sufrir una importante mediatización gubernamental, mal añadido al de las numerosas excepciones establecidas en favor de los ficheros de titularidad pública, que exigen una especial vigilancia.

En cuanto al Régimen Jurídico de la Agencia, el Estatuto establece su personalidad jurídica propia y plena capacidad pública y privada, y determina que ésta ejercerá sus funciones por medio del Director, por lo cual los actos de éste se consideran actos de la Agencia, y éstos agotan la vía Administrativa, Art. 2.4.

En lo que se refiere a las funciones de la Agencia, la razón de ser de ésta consiste en ofrecer las garantías específicas para el derecho a la autodeterminación informativa que deriva de su propia existencia, como institución independiente, cuya finalidad es velar por el respeto al sistema de protección de datos.[1]

■ 1 LUCAS MURILLO DE LA CUEVA, Pablo. Protección de Datos Personales ante el uso de la Informática en el Derecho Español. 1992.

Las funciones a través de las cuales se va a cumplir este cometido, así como las potestades de la Agencia son las siguientes:

*** Corresponde a la Agencia ejercer todas las funciones que le atribuye el Art. 36 de la LORTAD, que podrían encuadrarse en la siguiente clasificación:**

** *Función genérica de salvaguarda,* respecto a las derechos de información y defensa de los afectados.[2]

** *Función de integración normativa,* dictando instrucciones precisas, adecuadas a los principios marcados por la LORTAD.[3]

** *Función consultiva,* informando preceptivamente los proyectos de disposiciones que desarrollen la ley.

** *Función informativa,* personalizada, publicidad general acerca de los ficheros existentes, así como publicación anual de una Memoria que se remitirá al Ministerio de Justicia.[4]

** *Función contenciosa,* atendiendo las reclamaciones y peticiones de los ciudadanos interesados.

** *Función inspectora,* que permite a los responsables de los ficheros recabar la información necesaria, para supervisar el funcionamiento correcto de éstos.[5]

** *Función de control,* autorizando o cancelando los ficheros que no se ajusten a lo establecido en la LORTAD.

** *Función instructora y represiva,* ejerciendo la potestad sancionadora, que se prevé en el Título VII de la Ley[6] .

** *Función coordinadora y preventiva,* según se establece en los Arts. 40 y 41 de la LORTAD, respecto a los órganos de las Comunidades Autónomas.

- 2 Relaciones con los afectados, art. 4.1 y 4.2 del Estatuto de la Agencia de Protección de Datos.
- 3 Cooperación en la elaboración y aplicación de las normas, art. 5 de la Agencia de Protección de Datos.
- 4 Publicidad de los ficheros automatizados, art. 7 y 8 de la Agencia de Protección de Datos.
- 5 Sección 5ª del Estatuto de la Agencia de Protección de Datos. R.D. 428/1993.
- 6 Art. 29 del Estatuto de la Agencia de Protección de Datos.

** *Función de cooperación con los organismos internacionales,* así 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.[7]

En el Capítulo III, del Estatuto de la Agencia de Protección de Datos, se desarrolla la estructura orgánica de ésta, configurándose con tres órganos diferenciados, en el ejecutivo, el Director, en el consultivo, el Consejo, y a efectos de publicidad, el Registro General de Protección de Datos.

La figura del Director queda definida como la persona que dirige y representa a la Agencia, teniendo la consideración de alto cargo. Su nombramiento, se formalizará a través de Real Decreto en consejo de Ministros y deberá recaer en uno de los integrantes del Consejo Consultivo.

De las funciones del Director podemos distinguir o clasificar las siguientes:

* *Funciones de Dirección,*[8] entre las que están; dictar resoluciones, adopción de medidas cautelares, autorizaciones, etc.

* *Funciones de gestión,*[9] como la adjudicación de contratos, control económico-financiero de la Agencia, proposición de la relación de puestos de trabajo, etc. La mayoría de estas funciones de gestión pueden ser delegadas en el Secretario General de la Agencia.

Tanto la LORTAD, como el Estatuto de la Agencia coinciden en afirmar que el Director «ejercerá sus funciones con plena independencia y objetividad y no estará sometido a instrucción alguna»[10] , sin embargo no se asegura su inamovilidad, que podría ser la manera más adecuada de conseguir esa independencia. Así se prevé la posibilidad de que el gobierno lo cese anticipadamente[11] .

La Sección 3ª del Estatuto de la Agencia de Protección de Datos, está dedicado al Consejo Consultivo[12] , órgano colegiado de asesoramiento del Director.

- 7 Art. 13 del Convenio del Consejo de Europa de 28 de enero de 1981.
- 8 Art. 12 del Estatuto de la Agencia de Protección de Datos.
- 9 Art. 13 del Estatuto de la Agencia de Protección de Datos.
- 10 Arts. 35.2 de la LORTAD y 16 del Estatuto de la Agencia de Protección de Datos.
- 11 Art. 35.3 de la LORTAD.
- 12 Art. 37 de la LORTAD.

La propuesta y nombramiento de sus miembros, queda establecida en el Art. 37 de la LORTAD, y se reproduce en el Art. 19 del Estatuto, desarrollándose en éste, quien propone en el caso del representante de los usuarios y consumidores, que lo hará mediante terna el Consejo de éstos, y la propuesta del vocal del sector de ficheros privados, que la hará el Consejo Superior de Cámaras de Comercio Industria y Navegación, también mediante terna.

Estas propuestas serán elevadas al Gobierno a través del Ministerio de Justicia, así los miembros del Consejo Consultivo serán nombrados y cesados por el Gobierno.[13]

Así mismo el Estatuto regula en sus Arts. 20 y 21 los extremos referentes a la renovación, duración del cargo y vacantes del Consejo Consultivo.

En cuanto a su funcionamiento, el Consejo Consultivo debe ajustar sus actuaciones a las normas que sean de aplicación de la Ley 30/92 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

La Sección 4ª del Estatuto desarrolla el Art. 38 de la LORTAD, que remitía a vía reglamentaria la regulación del procedimiento de inscripción de los ficheros, tanto de titularidad pública como privada.[14]

A este órgano corresponde velar por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, haciendo así posible el ejercicio de los derechos de información, acceso, rectificación y cancelación.

Por último en lo que se refiere a los órganos de la Agencia, en la Sección 6ª del Estatuto se desarrollan las funciones de la Secretaría General, siendo de gran relevancia y trascendental importancia para el ciudadano, el que a parte de las funciones típicas de una Secretaría General, definidas en el Art. 30, como son funciones de apoyo y ejecución, se establezcan dentro del apartado de otras funciones, aquellas que van desde la creación de un fondo de documentación en materias de protección de datos, hasta la publicación de repertorios oficiales, organización de conferencias y seminarios. Y lo que es más, facilitar la información a que se refiere el Art. 4.1 del propio Estatuto.

En éste, se establece, que -**la Agencia de Protección de Datos informará a las personas de los derechos que la Ley les reconoce en relación con el**

- 13 Art. 19.3 del Estatuto de la Agencia de Protección de Datos.
- 14 Arts. 24, 25 y 26 del Estatuto de la Agencia de Protección de Datos.

tratamiento automatizado de sus datos de carácter personal y a tal efecto podrá promover campañas de difusión, valiéndose de los medios de comunicación social-.

Así queda garantizada la difusión de todo lo concerniente a este tema, extremo de gran importancia para cualquier norma que nos sea de aplicación, pero más aún en este caso en el que la novedad de la materia tratada exige que se de una información precisa al ciudadano que de otra forma no podrá ejercer los derechos reconocidos en la LORTAD y desarrollados en el Estatuto, de información, rectificación y cancelación de sus datos.

Además de la importancia de la labor de información, para el ejercicio de estos derechos, el funcionamiento de la Agencia va a depender en gran parte de la difusión que se haga de ella, de sus funciones, servicios, carácter, etc.

No se va a tratar de una divulgación más del contenido de la norma, el legislador a entendido que para que la Agencia pueda desarrollar su trabajo es imprescindible difundirlo, y por ello lo incluye en el Art. 4.1 y 31 del Estatuto.

Sirvan por ello estas notas para ayudar a esa divulgación, que entendemos imprescindible, de las funciones de la Agencia de protección de Datos como Ente encargado de materializar y desarrollar con su aplicación a la LORTAD.

Infracciones Administrativas y Penales en Relación con la Protección de Datos

CARLOS M. ROMEO CASABONA
Catedrático de Derecho Penal.
Decano de la Facultad de Derecho Universidad de La Laguna

I. La Protección de la Intimidad y de Otros Bienes Emergentes en Relación con las Nuevas Tecnologías de la Información y de la Comunicación.

1. El derecho a la intimidad en la actualidad

La preocupación por la protección jurídica de la intimidad se ha visto acrecentada en los últimos decenios al comprobar la multiplicación y potencialidad de los procedimientos susceptibles de vulnerarla, como son los medios técnicos de captación y transmisión de la imagen y del sonido, así como los de acumulación y procesamiento de la información en general y de los datos de carácter personal. Quizá debido a que la intensificación de este fenómeno ha sido relativamente reciente, no se ha sentido hasta el presente una especial necesidad de delimitar el concepto del objeto de tutela, con el fin de establecer los procedimientos de protección más adecuados. Por otro lado, las concepciones y relaciones sociales actuales han ido mermando paulatinamente el reducto de la esfera íntima: las exigencias derivadas de un mayor intervencionismo estatal al tiempo que la satisfactoria realización de las

libertades públicas, propias de un Estado social y democrático de derecho, han puesto en primer plano -frecuentemente en detrimento del derecho a la intimidad- la legitimidad de la captación cada vez mayor por parte de las administraciones públicas de información sobre aspectos más o menos íntimos o reservados de los ciudadanos con el fin de poder realizar sus funciones y prestar sus servicios de forma más eficaz, al igual que el derecho a la información y la libertad de expresión.[1] Por otra parte, en el sector privado también se ha percibido que la posesión de información o la posibilidad de acceso a la misma constituye un instrumento imprescindible para la realización con éxito de ciertas actividades, incluso aunque con ello se afecte a la esfera privada de las personas.

Ante esta realidad la delimitación de lo que constituye la intimidad se convierte en una necesidad insoslayable. Por tanto, su concepción patrimonialista o autonomista (el famoso derecho "a ser dejado solo", de la concepción decimonónica norteamericana), ha tenido que ir dejando paso a su clara adscripción como derecho inherente de la personalidad, incluso reforzado como derecho humano (así, la Declaración Universal de los Derechos Humanos de 1948, art. 12) o derecho fundamental (por ejemplo, la Constitución española de 1978, art. 18), pero que trasciende incluso al ejercicio de otros derechos públicos o privados. A esta característica hay que añadir la de su relatividad contextual y carácter difuso, su dinamicidad y potencialidad expansiva, así como el hecho de ser compartido en ocasiones, pues el acceso de terceros a la esfera íntima no hace perder necesariamente siempre esa naturaleza, en particular cuando el afectado se ha visto obligado a compartirla.

En síntesis podemos entender por intimidad aquellas manifestaciones de la personalidad individual (o familiar) cuyo conocimiento o desarrollo quedan reservados a su titular o sobre las que ejerce alguna forma de control cuando se ven implicados terceros (entendiendo por tales tanto los particulares como los poderes públicos)[2]. Consecuentemente el derecho a la intimidad supone también el reconocimiento de esa reserva o de ese control sobre terceros, debiendo resaltar que incluimos no sólo el conocimiento sino también el desenvolvimiento en sí mismo, lo cual amplía su ámbito y por ello puede ser objeto de debate, que soslayamos aquí. Es evidente que cuando el interesado no dispone de ningún mecanismo legítimo de control sobre terceros la mani-

■ 1 V. Carlos M. ROMEO CASABONA, *El derecho a la intimidad en la sociedad actual*, en "Boletín Fundesco", nº 128, 8 y s. (1992).

■ 2 Que no es fácil acotar el concepto material de intimidad en cuanto bien jurídico, lo ponen de manifiesto Aurora GARCIA VITORIA, *El derecho a la intimidad en el Derecho penal y en la Constitución de 1978*, Aranzadi, Pamplona, 1983, 17 y ss.; Pilar GOMEZ PAVON, *La intimidad como objeto de protección penal*, Akal, Madrid, 1989, 29 y ss.; Fermín MORALES PRATS, *La tutela penal de la intimidad: privacy e informática*, Ed. Destino, Barcelona, 1984, 118 y ss.

festación de la personalidad afectada ha salido de su esfera íntima, y que en este caso su protección sólo es posible en la medida en que se afecte a la propia imagen o al honor, que se encuentran muy estrechamente vinculados con aquélla, incluso se reconoce que tienen una zona común[3]. De la intimidad hay que distinguir la llamada privacidad, concepto introducido recientemente en nuestra legislación, en concreto en la Exposición de Motivos de la Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal de 1992 -de la que me ocuparé más abajo-, cuando expresa que "la privacidad constituye un conjunto, más amplio, más global [que la intimidad], 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". No podemos entrar ahora a un análisis crítico de este concepto, pero sí conviene señalar que esta concepción que se apunta es tan sólo una de las facetas que pueden ser vulneradas por la utilización abusiva de datos informatizados, así como que con ésta pueden atacarse también otros intereses personales del individuo más allá de la intimidad o de la privacidad así entendida, como es el ejercicio de determinados derechos fundamentales y libertades públicas, sin necesidad de acudir a un entrecruzamiento de datos, a los que me referiré más abajo.[4]

2. Los cauces de protección sectorial de algunas manifestaciones de la intimidad

La intimidad así entendida encuentra tres cauces principales de protección, con instrumentos jurídicos diversos en su naturaleza y alcance. De ellos vamos a ocuparnos a continuación, haciendo notar no obstante, que dado lo inevitable de la relatividad del objeto de protección a que aludíamos y su hasta cierto punto carácter difuso, su protección se concreta en ciertas manifestaciones de la personalidad, las más significativas, y que en ocasiones -en concreto, en relación con la protección de datos- va más allá de la intimidad, para acotar bienes jurídicos de próxima, pero diferente textura.

2.1. La protección de la intimidad en su manifestación como reducto de la personalidad

■ 3 V. MORALES PRATS, *La tutela penal de la intimidad: privacy e informática*, cit., 136 y ss.; Pablo LUCAS MURILLO DE LA CUEVA, *La protección de los datos personales ante el uso de la informática en el Derecho español*, en "Estudios de Jurisprudencia", nº 3, 15 (1992).

■ 4 Por tal motivo puedo adelantar ya que entiendo que no puede identificarse como bien jurídico básico protegido por la LORTAD esa privacidad 'reinterpretada' como equivalente al derecho a la autodeterminación informativa o libertad informática, según pretende, con loable criterio pragmático, LUCAS MURILLO DE LA CUEVA, *La protección de los datos personales ante el uso de la informática en el Derecho español*, cit., 18. Sin embargo, en mi opinión, la libertad informática abarca más que esa descripción de la privacidad que ofrece el legislador en la Exposición de Motivos, aspectos que, no obstante, LUCAS también integra acertadamente en dicha libertad o autodeterminación.

En primer lugar estarían las intromisiones ilegítimas en aquella esfera de la intimidad que queda directa y exclusivamente reservada al propio interesado (o a su familia), quien tiene en sus manos la decisión sobre la magnitud del ámbito protegido, dentro de ciertos límites. La protección de esta proyección de la intimidad en nuestra legislación corresponde en gran medida a la Ley Orgánica 1/1982, de 5 de mayo de 1982, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, cuyos arts. 7 y 8 señalan, respectivamente, cuáles son esas intromisiones ilegítimas y cuáles no lo son; ley que, por cierto, caracteriza estos derechos (por tanto, también el derecho a la intimidad personal y familiar) como irrenunciables, inalienables e imprescriptibles (art. 1. 3)[5].

En el ámbito penal podrían destacarse algunos delitos relativos al descubrimiento y revelación de secretos, en concreto cuando el hecho consiste en el apoderamiento de papeles o cartas de otro (art. 497 del Código Penal)[6] o en la interceptación de las comunicaciones telefónicas o captación del sonido con instrumentos técnicos, bien por particulares, bien por la autoridad, funcionario público o agente de los mismos (arts. 497 bis y 192 bis, respectivamente); incluso, en cierta medida, también los delitos de injurias (sobre todo el art. 458 nº 2) y de allanamiento de morada (art. 490) podrían afectar a la tutela de la intimidad, como también desde otra perspectiva, el delito sobre la protección de la correspondencia (el art. 192). Todos ellos -salvo los delitos de injurias- tienen en común que se protege el espacio físico o continente del disfrute de la intimidad.

Puesto que en cierta medida el delito de captación de las comunicaciones telefónicas privadas o del sonido con instrumentos técnicos pretende responder a la mayor vulnerabilidad de la intimidad en relación con ciertas tecnologías, es oportuno detenerse brevemente en el análisis de los efectos protectores que ha supuesto la introducción de los arts. 497 bis y 192 bis en el CP[7]. La primera duda surge sobre el alcance del bien jurídico protegido. Se está de acuerdo en que se protege la intimidad de las comunicaciones orales, y ello lo refrenda la alusión a la utilización de medios técnicos para la captación del sonido; sin embargo, cuando el primer inciso del art. 497 bis se refiere a las comunicaciones telefónicas, es cierto también que incluye en primer lugar y sin discusión la captación de conversaciones telefónicas, esto es, orales, pero

- 5 V. Jaime VIDAL MARTINEZ, *El derecho a la intimidad en la Ley Orgánica de 5-5-1982*, Ed. Montecorvo, Madrid, 1984.
- 6 Art. 497 del CP: "El que para descubrir los secretos de otro se apoderare de sus papeles o cartas y divulgare aquéllos será castigado con las penas de arresto mayor y multa de 100.000 a 2.000.000 de pesetas. Si no los divulgare, las penas serán de arresto mayor y multa de 100.000 a 500.000 pesetas (...)".
- 7 Por Ley Orgánica 7/1984, de 15 de octubre.

también otras comunicaciones, también telefónicas, que afectando a la intimidad (o a los secretos), consisten en la transmisión de escritos por medio del télex y el telefax, así como de datos entre dos terminales de ordenador, siempre que en todos estos supuestos se utilice la línea telefónica como vía de comunicación y transmisión entre remitente y receptor.

La acción típica la expresa el CP con interceptar las comunicaciones telefónicas de otros o utilizar instrumentos o artificios técnicos de escucha, transmisión, grabación o reproducción del sonido; por tanto, cualquier otro procedimiento de captación del sonido que no se valga de medios técnicos no está cubierto por el tipo penal. Es preciso actuar sin el consentimiento del interesado, esto es, de todos los que intervienen en la comunicación o conversación, salvo si el secreto o aspecto relativo a la intimidad afecta tan sólo a una de las partes y es la que presta el consentimiento. Sujeto activo del delito decíamos que puede serlo cualquiera (art. 497 bis), o únicamente la Autoridad, funcionario público o agente de éstos (art. 192 bis). El tipo subjetivo está constituido en ambos delitos por el dolo; además, el art. 497 bis requiere un elemento subjetivo de lo injusto (no exigido para la modalidad del art. 192 bis), consistente en la intención de descubrir los secretos o la intimidad de otros. Para que se produzca la consumación del delito es preciso interceptar la comunicación telefónica o captar el sonido por los medios indicados, no siendo suficiente la instalación de aparatos o instrumentos técnicos, sin perjuicio de su consideración para la existencia de la tentativa del delito. Divulgar o revelar lo descubierto o la información obtenida da lugar a un tipo agravado (art. 497 bis, último inciso, y art. 192 bis, párr. 2º). En cuanto a la grabación ilegal como medio de obtención de prueba, es decir, sin la debida autorización judicial, salvo lo previsto legalmente en desarrollo del art. 55.2 de la Constitución (art. 192 bis), se entiende que no es admisible ni el hecho ni el medio de prueba como tal[8].

A pesar de la cobertura que ha pretendido darse con estos delitos, se han detectado ya algunas carencias, como que no incluye la captación de la imagen por procedimientos técnicos, ni la de datos informáticos, utilizando para ello procedimientos técnicos o no, a salvo de la interferencia de los mismos a través de la línea telefónica, ya apuntada, sin perjuicio de que esa misma conducta realizada en otras líneas específicas de transmisión de datos difícilmente quedaría abarcada por el tipo. Por otro lado, y en este caso en relación con el tipo del art. 497 bis, tampoco se daría éste cuando se accede a conversaciones de otros sin la intencionalidad inicial específica de descubrir los secretos o la inti-

■ 8 V. art. 11. 1 de la Ley Orgánica del Poder Judicial; STC 29 noviembre 1984; Tomás LOPEZ-FRAGOSO ALVAREZ, *Las intervenciones telefónicas en el proceso penal*, Colex, Madrid, 94 y ss.

midad de otros (p. ej., de forma accidental), pero con posterioridad se revelan (o utilizan) por el mismo "captador" o por un tercero, lo que no ha de ser relativamente infrecuente en relación con los datos.

El Proyecto de CP de 1992 pretende colmar estas lagunas, ampliando y actualizando los tipos delictivos de los actuales arts. 497 y 497 bis, que se unifican en uno solo. El art. 198 del Proyecto[9] incluye ya la grabación (y transmisión) de la imagen o "de cualquier otra señal de comunicación"; se suprime la interferencia de las comunicaciones telefónicas, puesto que es suficiente con la mención a las conductas de captación del sonido; además del apoderamiento de papeles o cartas, del mismo modo que el CP actual, sin la menor duda inadecuado en la actualidad, añade "cualesquiera otros documentos o efectos personales". En cuanto al elemento subjetivo del injusto, es más correcto el texto previsto, al requerirse la finalidad de descubrir los secretos o vulnerar la intimidad de otro. A diferencia del Anteproyecto, que no lo mencionaba[10], el Proyecto de 1992 ha previsto la incriminación del comportamiento señalado más arriba, que no cubre el actual art. 497 bis, es decir, el que con conocimiento de ilícito origen y sin haber tomado parte en el descubrimiento, difunda o revele lo descubierto por terceros (art. 198. 3, p. 2º). En cuanto a las previsiones del Proyecto sobre la protección de datos, me ocuparé de ellas más abajo.

Por otro lado, el Proyecto de 1992 aporta otra novedad por lo que se refiere a la protección del derecho a la propia imagen como proyección de la intimidad, no sólo frente a la captación de la misma (art. 198), sino también frente a su utilización (o el nombre) sin el consentimiento del interesado con fines económicos (profesionales, comerciales o publicitarios).[11] Pretende así el Proyecto cubrir también una laguna sobre la protección penal de este derecho a la propia imagen, que estando bien protegido en el ámbito civil (LO 2/1982),

- 9 Dice así el art. 198: "1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apoderare de sus papeles, cartas o cualesquiera otros documentos o efectos personales, o utilizare instrumentos o artificios técnicos de escucha, transmisión o grabación del sonido, la imagen o de cualquier otra señal de comunicación, será castigado con la pena de prisión de seis meses a dos años y multa de doce a veinticuatro meses. 2. Las mismas penas se impondrán al que, sin estar autorizado, se apoderase de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o cualquier otro tipo de archivo o registro, público o privado. 3. Se impondrá la pena de prisión de uno a tres años si se difundieren o revelaren a terceros los datos reservados descubiertos a que se refieren los números anteriores. Será castigado con la pena de prisión de seis meses a dos años y multa de doce a veinticuatro meses, el que con conocimiento de su ilícito origen, y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior. 4. Si los hechos se realizaren por las personas encargadas o responsables de los ficheros, soportes informáticos, archivos o registros, se impondrá la pena de prisión de dos a cuatro años, y si difundieren o revelaren los datos reservados, se impondrá la pena de prisión de tres a cinco años".
- 10 V. art. 194 del Anteproyecto de CP presentado por el Ministro de Justicia en abril de 1992.
- 11 Art. 201: "1. El que utilizare, por cualquier medio, la imagen o el nombre de otra persona, sin su consentimiento, con fines profesionales, comerciales o publicitarios, será castigado con la pena de arresto de doce a veinticuatro fines de semana y multa de seis a doce meses (...)".

plantea dudas sobre el acierto de la misma, a la vista del principio de subsidiariedad, *ultima ratio* e intervención mínima del Derecho Penal.

2.2. Protección de la intimidad en su manifestación de confidencialidad compartida

En este ámbito se encuentran aquellos aspectos de la intimidad que por prescripción de la ley o por la propia naturaleza de las relaciones interindividuales o sociales facultan el acceso a terceros, pero que están obligados por ley a mantener su confidencialidad. De ello se deriva el deber del secreto profesional o el oficial de los funcionarios públicos, cuyo cumplimiento el afectado puede exigir, e incluso reclamar las responsabilidades a que hubiera lugar. La infracción del secreto profesional aparece con carácter general en el ámbito civil en la citada Ley Orgánica de 1982 (art. 7. 4), de forma sectorial en algunas leyes o disposiciones sobre materias administrativas[12] , mientras que en el penal sólo en algunos casos, como el del administrador, dependiente o criado en relación con los secretos de su jefe (art. 498)[13] , del abogado o procurador (art. 360) y de los funcionarios públicos (art. 364 y ss., 367)[14] .

El extendido sentimiento de que el secreto profesional ha de contar con una adecuada protección penal con carácter general, de la que carece en la actualidad nuestro CP (sin perjuicio de algunas excepciones, ya aludidas), es atendido por el Proyecto de CP de 1992 (art. 199)[15], manteniendo los delitos correspondientes cometidos por funcionarios públicos en términos semejantes al CP vigente (arts. 394 y ss.).

La novedad en relación con los primeros consiste en tipificar la revelación del secreto y específicamente la revelación de aquellos datos de las personas que deben considerarse secretos y que se han conocido en razón del oficio, trabajo dependiente o la profesión. Por lo que se refiere a ésta última, no cabe

- 12 V., p. ej., la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, art. 50. 2. a (infracción muy grave: el incumplimiento del deber del secreto estadístico).
- 13 Art. 498: "El administrador, dependiente o criado que en tal concepto supiere los secretos de su principal y los divulgare será castigado con las penas de arresto mayor y multa de 100.000 a 500.000 pesetas".
- 14 No se olvide tampoco el delito de vulneración de correspondencia privada (art. 192 CP, en especial el parr. 2º), ni desde otra perspectiva ajena a la intimidad, los delitos de descubrimiento y revelación de secretos e informaciones relativas a la defensa nacional (arts. 135 bis a, bis b, bis c y bis d; y arts. 53 a 56 del CP Militar). Por otro lado, la Ley 9/1968, de 5 de abril, reformada por Ley 48/1978, de 7 de octubre, sobre Secretos Oficiales.
- 15 Art. 199: "1. El que revelare los secretos ajenos, de los que tuviere conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de seis meses a dos años y multa de seis a doce meses. 2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgare los secretos de otra persona, será castigado con la pena de prisión de seis meses a tres años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años".

duda ya de la obligación impuesta penalmente a todos los profesionales. De todos modos, son aceptables excepciones, por lo general amparadas por la eximente de la responsabilidad de obrar en el cumplimiento de un deber (art. 8º nº 11 del CP vigente, art. 19 nº 8 del PCP 1992). Esta línea argumental permite dar un sentido más coherente a la redacción del Proyecto, que puede ser algo impreciso cuando dice: "El profesional, que con incumplimiento de su obligación de sigilo o reserva..."; pues no prejuzga cuál de las dos alternativas interpretativas es la correcta (sobre lo que no nos podemos detener ahora): si el PCP establece una obligación jurídica de secreto bajo amenaza penal, o tal obligación habrá que extraerla (y por tanto, también su infracción) de otros sectores del ordenamiento jurídico, en concreto de las disposiciones específicas sobre el secreto profesional.

2.3. La protección de la intimidad en relación con el procesamiento de datos a través de las nuevas tecnologías de la información

Por sus especiales implicaciones, podríamos mencionar aparte la protección de la intimidad en relación con ficheros o archivos, principalmente cuando han sido procesados informáticamente[16] . En estos casos el alcance de la intimidad se centra sobre todo, aunque no solamente (pues siguen vigentes algunos de los aspectos mencionados más arriba), en que el afectado debe aportar información privada o, incluso, reservada, que le concierne, pero se le reconoce una cierta capacidad de control sobre la misma. Dicho control puede consistir en la pertinencia o no de la información solicitada para el objetivo perseguido, que cuando entra de lleno en el núcleo de la intimidad (los llamados datos sensibles o supersensibles, relativos al origen racial, opiniones políticas, adscripciones sindicales, convicciones religiosas u otras convicciones, la salud, vida sexual), la aportación de información queda vedada, si no media el consentimiento del afectado, o muy limitada, y siempre con garantías reforzadas en cuanto a su utilización. Esta llamada intimidad informática, que, como decimos, abarca la reserva de los datos, confluye con la llamada libertad e identidad informáticas, que se refiere al control (sobre su exactitud, pertinencia, actualización, destino y uso, etc.) de los datos personales por parte del interesado, tengan o no carácter íntimo, por lo que conviene tener presente que son dos intereses de protección -bienes jurídicos- diferenciados[17] , aunque

- 16 V. Javier BOIX REIG, *Protección jurídico-penal de la intimidad e informática*, en "Poder Judicial", nº Especial IX, 39 y ss. (1989); Fulgencio MADRID CONESA, *Derecho a la intimidad, informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984; MORALES PRATS, *La tutela penal de la intimidad: privacy e informática*, cit., 45 y ss. y 289 y ss.; Esteban SOLA RECHE,*La protección penal de la intimidad informática*, en "Revista de la Facultad de Derecho de la Universidad de La Laguna", nº 11, 186 y ss. (1991).
- 17 V. LUCAS MURILLO DE LA CUEVA, *La protección de los datos personales ante el uso de la informática en el Derecho español*, cit., 17 y s.; Carlos M. ROMEO CASABONA, *Poder Informático y Seguridad Jurídica*, Fundesco, Madrid 1988, 33; SOLA RECHE,*La protección penal de la intimidad informática*, cit., 196

en ocasiones se solapen y confluyan, en gran parte como consecuencia de las facultades de control que suelen ser reconocidas al respecto.

La Constitución refrenda esta protección bifronte en el art. 18. 4, que se remite a una ley que limite 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*". Es en este último inciso, dentro de su ambigüedad, donde podemos extraer ese derecho fundamental a la libertad informática o autodeterminación informativa[18] , puesto que es cierto que el honor de las personas apenas si es susceptible de agresión mediante el uso de la informática, y ya hemos visto que la sola referencia a la intimidad tampoco permitiría cubrir de forma satisfactoria -salvo que se ampliase de forma excesiva su ámbito, con los riesgos inherentes de una mayor imprecisión de la que ya adolece, y consiguiente pérdida de su capacidad efectiva como objeto de protección jurídica- otros componentes de la protección de la esfera personal que se concretan en la libertad informática o autodeterminación informativa[19] .

El mandato constitucional, por fin cumplido por la Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)[20] , colma una importantísima laguna legal de nuestro ordenamiento jurídico ampliamente sentida por la opinión pública. Hasta entonces la protección civil en lo que se refiere tan sólo a la intimidad[21] la suministraba con carácter temporal la Ley de 1982, en su disposición transitoria primera, que ha sido derogada por la LORTAD, la cual dedica el art. 17 al derecho a ser indemnizados los afectados que como consecuencia del incumplimiento de lo dispuesto en dicha Ley por el responsable del fichero, sufran un daño o lesión en sus bienes o derechos, aunque no parece pertinente la limitación de responsabilidad a los comportamientos indebidos del responsable del fichero, que le hace acreedor en este sentido de una culpa *in vigilando* (en las Administraciones Públicas) o *in eligendo* (en el ámbito privado), sino también por parte de los empleados que no actúen de conformidad con aquél. Aparte de alguna dispo-

- 18 LUCAS MURILLO DE LA CUEVA, *La protección de los datos personales ante el uso de la informática en el Derecho español*, cit., 17, lo configura como un nuevo derecho fundamental deducible del art. 18. 4 de la CE.
- 19 V. más ampliamente en este sentido, aportando argumentos que comparto, LUCAS MURILLO DE LA CUEVA, *La protección de los datos personales ante el uso de la informática en el Derecho español*, cit., 14 y ss.
- 20 LO 5/1992, de 29 de octubre. Su entrada en vigor estaba prevista a los tres meses de su publicación en el Boletín Oficial del Estado (Disp. Final Cuarta; publicada en el BOE de 31 octubre 1992), es decir, desde el 1º de febrero de 1993. Debe mencionarse que esta Ley ha sido recurrida, por presunta inconstitucionalidad de alguno de sus preceptos, ante el Tribunal Constitucional.
- 21 Los demás comportamientos lesivos que no afectasen de forma clara a la intimidad podían solventarse como responsabilidad extracontractual a partir del art. 1902 del Código Civil, lo que no era siempre satisfactorio, puesto que la acreditación de los requisitos que le dan vida podían plantear serias dificultades, empezando por la demostración del perjuicio, el cual, como veremos más abajo, no es presupuesto ineludible para el régimen de infracciones de la LORTAD.

sición sectorial aislada referida a la actividad administrativa, la tutela de los datos se obtenía hasta la promulgación de esta Ley a través del Convenio del Consejo de Europa de 28 de enero de 1981, vigente en nuestro país (art. 96. 1 de la CE), sin entrar ahora en las serias reservas y polémica sobre su aplicabilidad directa o, cuando menos limitada, que suscitó[22] , puesto que obligaba a un desarrollo legal interno (art. 4º). También habrá que tener presente en su momento la (todavía, según nuestras noticias) Propuesta de Directiva de la Comunidad Europea, sobre la misma materia. La legislación no penal en materia de protección de datos cumple, o ha de cumplir, una función eminentemente preventiva de abusos en relación con la utilización de aquéllos, fundamentalmente, lo que implica la adopción de medidas sobre la obtención, tratamiento, utilización y cesión de los datos.

2.3.1. La protección de los datos: régimen de las infracciones administrativas en la Ley Orgánica de protección de datos de carácter personal

La protección de los datos de carácter personal que pretende garantizar la LORTAD parece tener presente estos bienes jurídicos: intimidad (intimidad informática, diríamos), libertad e identidad informáticas, además del reiteradamente mencionado libre y pleno ejercicio de los derechos de las personas.[23] En efecto, estas ideas se pueden extraer tanto de los "principios de la protección de los datos" (Título II, arts. 4 a 11) como de los "derechos de las personas" (Título III, arts. 12 a 17). La primera faceta, la protección de la intimidad en relación con los datos, se sustenta sobre todo en el reconocimiento del carácter reservado de los mismos, lo que conduce a la consagración específica del deber de secreto (arts. 10, y 39. 2) y al establecimiento de infracciones relativas al incumplimiento de tal deber, como grave (art.43. 3. g) o muy grave (art. 43. 4. g). Este es precisamente el bien jurídico que ha merecido la atención del Proyecto CP 1992, tanto en relación con los datos (art. 198) como, en sentido más amplio, el secreto profesional (art. 199). La segunda faceta se refiere a la identidad y libertad informáticas, como se desprende del reconocimiento a los afectados del derecho de información y acceso a los datos y del derecho de rectificación y cancelación, así como de los principios relativos a la calidad de

- 22 V., p. ej., Carlos M. ROMEO CASABONA, *Poder Informático y Seguridad Jurídica*, Fundesco, Madrid 1988, 32. A este respecto, y en la misma línea, la STS (3ª) 30 abril 1990 señaló: "La aplicación directa del Convenio de 28 de enero de 1981... se halla supeditada, como establece su artículo 4.1., a la adopción por cada Parte, en su derecho interno, de las medidas necesarias para que sean efectivos los principios básicos para la protección de datos a que se refiere el Convenio, previsión coincidente con la del artículo 94.1 e) de la Constitución Española sobre la posible exigencia de medidas legislativas para la ejecución de los Tratados o Convenios".
- 23 No obstante, la LORTAD se propone un objetivo más amplio, marcado por la Constitución: "La presente Ley Orgánica, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizados de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos" (art. 1º).

los datos, a la información sobre su recogida, al consentimiento, a la seguridad y a la cesión de los mismos. También aquí se prevén numerosas infracciones que pretenden garantizar esos derechos y principios que afectan en síntesis a lo que denominamos la identidad y libertad informática. Y, finalmente, con todo este arsenal de garantías y derechos se establece un marco para que el tratamiento automatizado de los datos de carácter personal, cuando resulte necesario, no menoscabe el libre y pleno ejercicio de otros derechos cívicos o políticos de las personas reconocidos por la Constitución.

Lo que podríamos denominar sujeto activo de las infracciones administrativas previstas por la Ley afecta de modo exclusivo a los responsables de los ficheros; ellos, señala la Ley, están sometidos a su régimen sancionador (art. 42. 1). Resulta llamativa esta restricción, puesto que el responsable del fichero es una categoría jurídica que la propia Ley define y acota (art. 3. d), siendo que otros empleados del fichero pueden ser materialmente infractores, y, por ejemplo, a ellos alcanza también de modo expreso el deber de secreto que la Ley impone (art. 10), como también a los funcionarios que ejerzan la inspección de los ficheros, que de este modo queda sin respuesta sancionadora, sin perjuicio de las indemnizaciones que se puedan reclamar por los procedimientos previstos (art. 17. 3). En realidad, cuando las infracciones son cometidas en el seno de las Administraciones Públicas el régimen sancionador se traslada al ámbito disciplinario de las mismas (arts. 42. 2 y 45. 2), por lo que el catálogo de sanciones que prevé la Ley sólo es aplicable a los responsables de ficheros de titularidad privada. Además, mediante resolución del órgano competente, al que aludiremos a continuación, se establecerán las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción cometida en el seno de las Administraciones Públicas. Quedan excluidos del régimen de infracciones y sanciones (esto es, del Título VII de la Ley) los ficheros pertenecientes a las Cortes Generales, al Tribunal Constitucional, al Tribunal de Cuentas, al Defensor del Pueblo y al Consejo General del Poder Judicial (Disp. Adicional 1ª), para los que rigen, no obstante, las garantías que la Ley acoge para los principios y derechos de las personas.

Por otro lado, la potestad sancionadora se encomienda a la Agencia de Protección de Datos (art. 36. g), contra cuyas resoluciones cabe recurso contencioso-administrativo (art. 47. 2). A este respecto, el Estatuto de la Agencia de Protección de Datos[24] reitera estas competencias (art. 12. 2. i y j), incluida la adopción de medidas cautelares y provisionales que requiera el ejercicio de la potestad sancionadora de la Agencia con relación a los responsables de los ficheros privados (art. 12. 2. h), mientras que los actos de instrucción relativos

■ 24 Aprobado por R.D. 428/1993, de 26 de marzo.

a los expedientes sancionatorios en relación con esto último corresponde a la Inspección de Datos (art. 29). En cuanto a los ficheros de titularidad pública, ya se ha indicado su remisión al régimen disciplinario de los funcionarios, de acuerdo con la legislación vigente. Sin embargo, la Ley señala que el Director "podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran". Ese "podrá" parece dejar su discreción tal proposición, lo que resultaría comparativamente injusto en relación con los responsables de ficheros privados. En esta materia incumbe al Director de la Agencia determinadas obligaciones de comunicación, como notificar al responsable del fichero de titularidad pública, al órgano del que dependa jerárquicamente y a los afectados si los hubiera, de la resolución sobre las medidas que procede adoptar (art. 45. 1), así como sobre la misma y las demás actuaciones al Defensor del Pueblo (art. 45. 4). Por su parte, el Director de la Agencia debe ser informado sobre las resoluciones que recaigan (se entiende que por parte de las Administraciones Públicas competentes) en relación con las medidas y actuaciones adoptadas por él mismo (art. 45. 3).

La Ley distribuye las infracciones en leves, graves y muy graves (art. 43.1), describiendo hasta un total de veintiuna. Estas son las infracciones que establece la LORTAD en su art. 43:

"1. Las infracciones se calificarán como leves, graves o muy graves.

2. *Son infracciones leves:*

a) No proceder, de oficio o a solicitud de las personas o instituciones legalmente habilitadas para ello, a la rectificación o cancelación de los errores, lagunas o inexactitudes de carácter formal de los ficheros.

b) No cumplir las instrucciones dictadas por el Director de la Agencia de Protección de Datos, o no proporcionar la información que éste solicite en relación a aspectos no sustantivos de la protección de datos.

c) No conservar actualizados los datos de carácter personal que se mantengan en ficheros automatizados.

d) Cualquiera otra que afecte a cuestiones meramente formales o documentales y que no constituya infracción grave o muy grave.

3.- *Son infracciones graves:*

a) Proceder a la creación de ficheros automatizados de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.

b) Proceder a la creación de ficheros automatizados de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible, o sin proporcionarles la información que señala el artículo 5 de la presente Ley.

d) Tratar de forma automatizada los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidas en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio del derecho de acceso y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto, cuando no constituya infracción muy grave.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria, se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

4. *Son infracciones muy graves:*

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar de forma automatizada los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar de forma automatizada los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente o violentar la prohibición en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos automatizados de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia, temporal o definitiva, de datos de carácter personal que hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar de forma automatizada los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7."

En síntesis, podríamos agrupar esta larga enumeración de infracciones atendiendo a varios criterios, así: a) atendiendo a los principios de protección infringidos: sobre la calidad de los datos (apartados. 2.c, 3.f y 4.a); sobre el derecho de información en la recogida de datos (ap.3.c); sobre el consentimiento (ap. 3.c); sobre datos especialmente protegidos (ap. 4.c); sobre la seguridad de los datos (ap. 3.h); sobre el secreto (aps. 3.g y 4.g); sobre su cesión (ap. 4.b);

b) derechos de las personas infringidos: sobre información y acceso (ap. 3.e); sobre rectificación y cancelación (aps. 2.a y 3.f); c) contra las funciones y competencias de la Agencia de Protección de Datos (aps. 2.b, 3.i y 3.j); d) sobre los requisitos de creación de ficheros e iniciación de recogida: de titularidad pública (ap. 3.a); de titularidad privada (ap.3.b); e) sobre el movimiento transfronterizo de los datos (ap. 4.e).

En cada una de las clases de infracciones aparece una de éstas descrita en términos muy amplios, que parece tener una función de recogida o "escoba", dentro de su categoría. Así, como infracción leve: "cualquiera otra que afecte a cuestiones meramente formales o documentales y que no constituya infracción grave o muy grave" (art. 43.2.d); como infracción grave: "tratar de forma automatizada los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidas en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave" (art. 43.3.d); y muy graves: "tratar de forma automatizada los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales" (art. 43.4.f). Sin embargo, las dos últimas presentan en algunos casos un solapamiento con otras infracciones más perfiladas dentro de su respectiva categoría, lo que no sucede con la infracción leve.

Las sanciones previstas son pecuniarias (art. 44), pero consideramos excesivamente elevado el tope mínimo establecido para las sanciones aplicables a las infracciones leves (100.000 pesetas), teniendo en cuenta el criterio de proporcionalidad exigible en relación con éstas. La graduación de la cuantía de las sanciones se hará atendiendo a los siguientes criterios (art. 44. 4): a) la naturaleza de los derechos personales afectados, que parece aludir a los derechos de esta clase que así identifica la propia Ley en su Título III, a pesar de que las vulneraciones a los principios recogidos en el Título precedente (que también pueden dar lugar a infracciones) pueden revestir especial gravedad para los afectados, motivo por el cual hay que desechar tal interpretación restrictiva y extenderla también a los principios de protección de los datos siempre que consagren derechos individuales en relación con los datos (consentimiento, secreto, etc.); b) el volumen de los tratamiento efectuados; c) el grado de intencionalidad, que ha de vincularse a la comisión dolosa o imprudente, quedando excluido el acaecimiento fortuito, por ser contrario al principio de culpabilidad[25] ; d) la reincidencia, la cual habrá de entenderse en sentido téc-

■ 25 Téngase en cuenta la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Común, art. 130, si bien marca el límite mínimo del principio de "responsabilidad" en la simple inobservancia (art. 130. 1).

nico-jurídico administrativo (y no penal, art. 10. 15)[26] , pero, por razones obvias, sólo afecta a la comisión previa de alguna infracción de las previstas en la Ley, cualquiera que sea su gravedad, pues mantienen la misma naturaleza a pesar de su posible diferencia de gravedad, siempre que hubiera recaído ya sanción por la anterior o anteriores. De todos modos, la Agencia de Protección de Datos tiene la potestad de la inmovilización de los ficheros en algunos casos, con la sola finalidad de restaurar los derechos de las personas afectadas (art. 48), medida por tanto cautelar, no sancionatoria. Como se ve, no se ha previsto como sanción la cancelación o clausura definitiva del fichero, que sería altamente perturbador para el cumplimiento de sus funciones y prestación de servicios si es de titularidad pública, pero tampoco si es privado, medida que sería igualmente perturbadora, pero en todo caso es discutible la renuncia a tal sanción, en casos especialmente graves, como, p. ej., en relación con ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, religión, creencias, origen racial o vida sexual, expresamente prohibidos por la Ley (art. 7. 4).

El art. 47 remite para el procedimiento sancionador a un futuro desarrollo reglamentario. También se prevén los plazos para las prescripción de las infracciones y sanciones, de acuerdo con su diferente gravedad respectiva (art. 46).

Una cuestión pendiente sería reflexionar sobre la oportunidad político-criminal de que aquellas infracciones especialmente graves pasaran a constituir delitos en el futuro CP, pero, como veremos a continuación, no ha sido éste el entendimiento de los redactores del Proyecto, puesto que sólo ha criminalizado en relación con la LORTAD la infracción del secreto y el apoderamiento de los datos.

Por último, algunas de las numerosas previsiones de desarrollo reglamentario afectan a la posibilidad de sustanciación efectiva de las sanciones correspondientes a la infracción cometida, por lo que que tal desarrollo es decisivo para la eficacia real futura de la potestad sancionadora, como lo ha sido ya, p.ej., el R.D. sobre la estructura orgánica de la Agencia de Protección de Datos, pero aún quedan materias pendientes (las infracciones de los aps. 3. d, 3. h, 3. i, del art. 43; el procedimiento a seguir para la determinación de las infracciones y la imposición de sanciones que incluye la Ley, art. 47. 1, etc.).

2.3.2. La protección penal de los datos de lege data y de lege ferenda

■ 26 Art. 131. 3. c, de la Ley de Régimen Jurídico: "La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme".

Por lo que se refiere a la protección penal de los datos informatizados, ésta es nula mientras no se reflejen en papeles o cartas susceptibles de apoderamiento (art. 497 CP), o no se intercepten en el curso de su transmisión de un terminal a otro por cable -línea- telefónico, si se acepta la propuesta interpretativa sugerida más arriba del art. 497 bis CP, sin perjuicio de que si son autores los funcionarios públicos puedan ser castigados más fácilmente a través de los delitos que protegen el deber de secreto de éstos. En consecuencia, es deseable e inevitable la incorporación al CP de algún delito sobre esta materia, en relación con el cual el principio de intervención mínima debe aclarar que formas de agresión contra qué aspectos de los que son portadores los datos merecen protección penal y cuáles no.

Por su parte, el Proyecto de Código Penal de 1992 prevé un delito relativo al apoderamiento sin autorización de datos reservados de carácter personal o familiar de otro registrados en ficheros, soportes informáticos o cualquier otro tipo de archivo o registro, público o privado (art. 198. 2). Contamos ya con los antecedentes del Proyecto de 1980 (art. 199) y de la Propuesta de 1983 (art. 189), pero, en principio, la conducta típica queda mejor definida en la versión del Proyecto, aunque persiste una remisión implícita a la Ley Orgánica sobre regulación del tratamiento automatizado de los datos de carácter personal (art. 3, d, y 11) cuando se alude "al que sin estar autorizado". Por cierto, la delimitación del sujeto activo requiere una interpretación, puesto que existe un tipo agravado (art. 198.4) cuando los hechos sean realizados por las personas responsables o encargadas de los ficheros, soportes informáticos, etc. En efecto, y como hemos indicado más arriba, la LORTAD define al responsable del fichero; sin embargo, en el Proyecto alude, por un lado, al responsable del fichero, que debería identificarse con el que define aquella Ley, pero extiende ese responsable a soportes informáticos y a otros archivos, que no encajan en tal definición; por otro lado, equipara a él a la persona encargada, para la cual no contamos con ninguna ayuda interpretativa en la citada Ley. Para diferenciar ambas categorías, responsable sería el que lo sea jurídicamente y encargado el que asuma las mismas funciones material o fácticamente; en ambos casos con competencia para acceder, manejar y copiar o ceder los datos y los ficheros y demás continentes que señala el Proyecto. Por fin, para el tipo básico quedaría la persona no autorizada empleada en el fichero o archivo que no tiene reconocidas competencias de copia o cesión o un tercero completamente ajeno al fichero. De todos modos, queda la duda de si puede haber alguien que se apodere de los datos reservados estando autorizado; no, pues apoderarse hay que entenderlo como tomarlos para sí, completamente distinto a cederlos a otro (entiéndase a otro fichero) en los supuestos permitidos por la Ley, y no creo que haya nadie que pueda estar autorizado para apoderarse de los datos reservados, pues no lo prevé la Ley. Finalmente, el responsable del fichero puede

ser una persona jurídica (art. 4.d de la LORTAD), por lo que entrará en juego la figura del que actúa en lugar de una persona jurídica (art. 15 bis del CP vigente y art. 28 del Proyecto).

También pueden plantearse problemas concursales (de normas) entre estos delitos (art. 198) y los de revelación de secretos (art. 199), en particular cuando el autor de los hechos relativos a la divulgación de los datos está comprendido entre las personas a las que la LORTAD obliga al secreto (art. 10).

Por otro lado, el Proyecto contrae su protección a la intimidad personal o familiar, en cuanto que la acción ha de recaer sobre "datos reservados", habiendo renunciado, por consiguiente, a otras manifestaciones de la protección de los datos, como son las ya aludidas identidad informática, que garantiza no sólo -como bien instrumental- la libertad informática sino el libre ejercicio de otros derechos y libertades públicas de los individuos; ello contrasta con la Propuesta de CP 1983, que incluía la manipulación de la información obtenida. Por consiguiente, y en los términos expuestos, se encomienda de forma exclusiva a la LORTAD los mecanismos preventivos frente a éste y otros comportamientos abusivos. Sin embargo, parece insuficiente el planteamiento actual del Proyecto de CP, al menos en relación con dos comportamientos especialmente graves, que pueden afectar no sólo a la intimidad, sino también a otras facetas de los datos personales: la utilización de los mismos por el que acceda a ellos sin autorización, aunque sea para sí, puesto que el "apoderarse" con que se describe la acción típica es dudoso que cubra la sola utilización de los datos, en el sentido de mera captación intelectual de su contenido y significado y no su aprehensión material; así como la alteración intencionada de los datos personales, dada la potencialidad altamente dañosa que implica este comportamiento. No creo que con ello se rebase el principio de intervención mínima, ni que en atención a este principio sea conveniente introducir otros hechos, que, como hemos visto, tienen la cobertura adecuada como infracciones administrativas en la LORTAD. Por consiguiente, el art. 198. 2 debería concluir con la siguiente frase: *"o los utilizare o modificare en perjuicio de otro"*. Con la presencia del elemento subjetivo se restringiría suficientemente el delito.

Por otro lado, debería establecerse un *tipo culposo* para el encargado o responsable del fichero, además de los comportamientos dolosos cometidos por éstos que se recogen (art. 198. 4), cuando los hechos dolosos a que alude el art. 198 fueran cometidos por terceros como consecuencia de imprudencia grave de dicho encargado o responsable, de modo semejante al delito que se establece en otro lugar para la autoridad o el funcionario en relación con los secretos (art. 399).

Una novedad que debe recibirse favorablemente es que el Proyecto amplía la protección de los datos reservados a los que pertenecen a personas jurídicas: "Lo dispuesto en este Capítulo será aplicable al que descubriere o revelare datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código". Como decimos, es acertada la extensión a las personas jurídicas, pero queda en el aire cuál es en realidad el bien jurídico protegido en este delito, si la intimidad de las personas jurídicas o más bien el secreto de los aspectos internos de la misma, por el mero hecho de ser reservados.

2.4. Perspectivas

Para terminar señalemos que el concepto de intimidad está todavía lejos de haber sido acuñado con claridad, puesto que es muy evolutivo al hallarse condicionado por el contexto histórico, social, cultural y tecnológico. Por otro lado, parece imprescindible deslindar con la máxima nitidez posible, la intimidad de la privacidad, así como los derechos y bienes emergentes en relación con los datos informatizados de carácter personal, para lo cual es preciso un detallado estudio de la LORTAD, pero cuyos perfiles han sido cuando menos apuntados en este trabajo. Y, paradójicamente, frente a la creciente voracidad social sobre el acceso a las parcelas más reservadas del individuo, como hemos visto justificada dentro de ciertos límites, como consecuencia inevitable del ejercicio de las libertades públicas del Estado Democrático de Derecho y del funcionamiento eficaz del Estado Social, presenciamos una tendencia cada vez más firme de garantizar el derecho a la intimidad personal y familiar, manteniendo un núcleo exclusivo, así como mecanismos de protección para su ámbito compartido, lo que, por cierto, no es sino otra consecuencia del Estado Social y Democrático de Derecho.

Panorama de la Legislación Europea sobre Protección de Datos Personales

STEWART H. DRESNER
Licenciado en Ciencias Políticas y Marketing.
Universidad de Lancaster (Reino Unido).
Director de Privacy Laws & Business.
(Traducido por SANTIAGO RIPOLL CARULLA)

Introducción.

1. El pasado 15 de enero, en Madrid, tres personas fueron arrestadas por la policía acusadas de estar involucradas en la venta de datos personales procedentes del Centro de Informática del Departamento de Trabajo y de Seguridad Social.

El banco de datos del que disponían contenía información de más de 2 millones de ciudadanos españoles, y hacía referencia, entre otros, a los siguientes aspectos: D.N.I., sexo, estado civil, nombre y dirección, datos familiares (por ejemplo, número, edad y sexo de los hijos), nivel de ingresos, información sobre la vivienda y otros gastos, etc.

En mi intervención trataré de exponer el modo en que una actividad de este tipo estaría regulada por las leyes de protección de datos en la mayoría

del resto de paises europeos, así como la importancia de los principios contenidos en la Convención del Consejo de Europa sobre protección de datos.

Por supuesto que, dado que este escándalo ha producido un considerable impacto en la opinión pública española, es posible deducir de él algunas consecuencias positivas:

-Se ha adquirido conciencia de la necesidad de poseer una efectiva regulación de los datos personales;

-Ha permitido advertir la conveniencia de ampliar a través de una ley el contenido de la protección dispensada en esta materia por el artículo 18 de la Constitución española;

-Ha concienciado al Gobierno y al Parlamento de la importancia de contar con una adecuada legislación en materia de protección de datos, provocando una agilización en sus tareas al respecto.

2. Obviamente, en países que ya contaban con legislación sobre protección de datos ha habido también escándalos similares al ocurrido en España. Así, el asunto Burberrys, acaecido en Francia. Burberrys, la firma británica de confección de prendas de ropa de alta calidad, creó un banco de datos de sus clientes con el objetivo de informarles puntualmente sobre sus nuevos productos.

Cuando estas listas fueron empleadas por un candidato de extrema derecha en unas elecciones municipales para formalizar un mailing sobre su candidatura, fueron decomisadas por la Autoridad Francesa de Protección de Datos (Comission National Informatique et Libertés, CNIL) por no haber sido empleadas con la finalidad para la que se recopilaron inicialmente.

En buena lógica, no fue suficiente defensa para Burberrys el argumentar que el perfil de sus clientes (varones de elevada posición social) emparejaba bien en principio con los potenciales votantes del partido en cuestión.

La ley de protección de datos francesa contiene un principio esencial, el deber de informar al momento de la colecta de los datos de la finalidad para la que se emplearan.

3. Este episodio, pues, sirve para ejemplificar como el derecho de la protección de datos desplaza el punto de equilibrio desde la industria y los gobiernos a aquellos individuos cuyos datos son recolectados, almacenados y

procesados. Esta nueva situación resulta cuando menos incómoda para las empresas y las autoridades gubernamentales, acostumbradas a contar con altísimos niveles y con poderosos mecanismos de obtención de información relativa a sus ciudadanos y clientes en aras - se argumenta - de una mayor eficacia en su gestión.

Sin embargo, conviene mirar más allá de estas incomodidades inmediatas y proteger, así, la dignidad del individuo.

I. Las leyes europeas de protección de datos.

4. En el cuadro número 1 se recoge de forma gráfica el panorama de las leyes europeas de protección de datos. Por el momento, no nos detendremos en un examen profundo de este cuadro. Es suficiente con advertir que, aunque existen algunos principios comunes a estas leyes, también hay diferencias entre ellas.

Idéntico ejercicio debe realizarse en relación al cuadro número 2, donde el lector encontrará la totalidad de los proyectos de ley existentes actualmente en Europa.

Consideremos esta información desde una nueva perspectiva: los cuadros 3 y 4 reflejan los países europeos que cuentan ya con ley de protección de datos o bien que han elaborado un proyecto de ley sobre la materia, respectivamente.

En relación a los primeros, cabe indicar que Suecia fue el primer Estado en elaborar una normativa sobre la materia (1973), mientras que Holanda (1988) y Portugal (1991) han sido los últimos en hacerlo. Por otra parte, puede avanzarse que a finales de 1992 Bélgica, España e Italia verán aprobados sus respectivos proyectos de ley, de modo que el próximo año prácticamente todos los miembros de la Comunidad Europea (excepción hecha de Grecia) tendrán legislación sobre el tema. Esta normativa, por lo demás, se verá complementada con una Directiva comunitaria, cuyos postulados obligarán a cualquier organización que recopile y procese datos personales en un país miembro.

Procedamos a un examen algo más detallado de las diferentes leyes europeas de protección de datos personales.

5. En primer lugar, cabe indicar que su principal punto en común es el que todas ellas regulan el tratamiento de los datos automatizados o procesa-

dos, sin detenerse, pese a ello, en consideraciones sobre las características del proceso de informatización.

Todas las leyes:

-protegen a los individuos, entendiendo por éstos tanto a las personas físicas como a las jurídicas,

-reconocen el derecho de acceso y rectificación,

-establecen un sistema de recursos, de forma que si un individuo ve dañados sus intereses cuenta con mecanismos para obtener una compensación. A diferencia de la legislación estadounidense, las leyes europeas recogen la figura de la Autoridad de Protección de Datos, que hace las veces de ombudsman en la materia. Asimismo, los tribunales nacionales están capacitados para sancionar a las organizaciones públicas o a las compañías privadas que vulneren la ley.

6. La Convención del Consejo de Europa sobre protección de datos establece los principios que han de caracterizar a las legislaciones europeas. Éstos son susceptibles de ordenarse en tres grupos:

Derechos de los individuos:

-el derecho a conocer la existencia de un fichero que contenga información sobre uno mismo,

-el derecho de acceso a tal fichero;

-el derecho a exigir la corrección de los datos erróneos.

2. Responsabilidades de los titulares del fichero:

-recolección imparcial y legal de los datos,

-garantía de que la recopilación y el almacenamiento de los datos se realiza con una finalidad legítima y concreta, y que la información no es empleada con fines ajenos a los especificados,

-adecuación entre los objetivos a alcanzar con la configuración del banco de datos y el número y la calidad de los datos recopilados,

-exactitud de los datos y, cuando sea necesario, puesta al día de los mismos,

-obligación de destruir los datos personales contenidos en el fichero cuando ya no resulte necesario su almacenamiento.

3. Deberes de los usuarios:

-el responsable del fichero debe ser fácilmente identificable, lo que en la práctica se traduce en que sea conocido por el personal de recepción o por los miembros de la asesoría jurídica de la empresa,

-el acceso a los ficheros por parte de los individuos afectados no debe ser oneroso. En muchos Estados, la normativa impone la obligación de abonar a la empresa una cuota por disco consultado. Esta cuantía únicamente será devuelta en el supuesto de que el individuo advierta un error en la información,

-cualquier corrección que se realice deberá notificarse a la fuente de la que se obtuvieron los datos, para evitar así que se perpetúen los errores,

-instauración de un régimen de recursos y sanciones, que se entiende esencial para corregir posibles injusticias.

7. Junto a estos elementos comunes, las leyes europeas presentan también ciertas diferencias. En nuestra exposición nos referiremos tan sólo a algunas de ellas. Así, las legislaciones de algunos Estados atienden no sólo las bases de datos automatizadas, sino también los ficheros manuales, ya que se entiende que la garantía de los principios indicados no depende solamente de los mecanismos de recopilación y ordenación de los datos.

En cualquier caso, incluso en este grupo de leyes, los requisitos que se exigen de cara al registro de los datos únicamente se predican de los ficheros automatizados, nunca se hacen exigibles a los bancos de datos manuales.

Quizás, aquellos de Uds. que estén más familiarizados con el tema se hayan sorprendido de que no me haya referido hasta este momento al tema del registro. La razón es que este enfoque - que ciertamente ha sido el más usual mientras los objetivos perseguidos por las diferentes leyes era ordenar los procedimientos de recopilación masiva de información - resulta en la actualidad algo desfasado. Con todo, dado que la mayoría de las leyes europeas sobre protección de datos actualmente en vigor se basan en este modelo, expondré brevemente las características de lo que podemos

denominar el modelo sueco, inspirador de la primera generación de leyes sobre la cuestión.

II. El modelo sueco.

8. Suecia fue el primer Estado en contar con una normativa que cubriera a la vez los bancos de datos del sector público y del sector privado. Para comprender esta opción recordemos el contexto en que se aprobó la ley sueca en 1973.

En tal fecha, el principal problema estribaba en el hecho de que los datos personales se almacenaban en grandes ordenadores centrales, de modo que resultaba muy difícil determinar la presencia de una información. Incluso cuando se conocía que esta información además de almacenada había sido ordenada de un modo u otro - configurándose así, por ejemplo, ficheros policiales o de carácter fiscal, en el sector público, o bancos de datos relativos a la situación laboral de los empleados de una empresa o a la situación crediticia de los clientes de un banco, en el sector privado -, resultaba imposible acceder a ella. Lo que es peor ni tan siquiera existían mecanismos que garantizaran a los individuos afectados el derecho a acceder a esta información. Paralelamente, las empresas y organismos públicos se consideraban titulares exclusivos, propietarios de los ficheros así estructurados, de suerte que consideraban que un acceso a ellos resultaba un menoscabo a sus derechos de propiedad.

El modelo sueco de un sistema de registro masivo fue diseñado precisamente para dar nuevos derechos a los particulares afectados, y para imponer nuevas responsabilidades a las organizaciones del sector, fueran éstas públicas o privadas. En definitiva, se trataba de asegurar:

-un registro central de todos los bancos de datos del país;

-la Autoridad de Protección de Datos es la única con potestad para permitir a los responsables de los bancos de datos existentes el configurar ficheros a partir de determinados datos (raza, religión, conductas sexuales...), que se consideraran sensibles;

-los particulares tienen derecho a informarse sobre los datos que cada organización posee sobre ellos;

-los particulares tienen derecho a comprobar si una organización ha creado un fichero sobre ellos;

-los particulares tienen derecho de acceso a los ficheros relativos a su persona;

-los particulares tienen derecho a exigir la rectificación de la información errónea, o cuando menos a incluir en el disco su versión.

Junto a estos derechos y obligaciones, la Autoridad de Protección de Datos posee ciertos poderes que vienen sugeridos por su propia denominación, Datainspektionen, u Oficina de Inspección de Datos. Así, tiene capacidad para visitar los locales de las empresas del sector, incluso sin previo aviso, y para formalizar una inspección de los sistemas de seguridad del software, de la formación del personal,... Estas visitas de inspección pueden llevarse a cabo bien a instancias de la Oficina de Inspección, bien a raíz de una reclamación.

9. Este modelo tuvo una gran influencia y a semejanza suya fueron adoptadas las leyes de protección de datos adoptadas durante el año 1978 - Francia, Dinamarca, Noruega y Austria -, así como la legislación vigente desde 1979 en Luxemburgo, las normas adoptadas en Israel e Islandia en 1981, en el Reino Unido (1984), la Isla de Man y Guernsey (1986), y en Jersey (1987).

Desde hace unos diez años, pues, ha quedado establecido el modelo de legislación en la materia. Desde entonces la principal cuestión radicaba en averiguar cuál sería la próxima normativa aprobada y qué ligeras variaciones presentaría. La ley de protección de datos alemana, de 1977, resultaba ser la única excepción a esta situación, pues los mecanismos de garantía de la aplicación de los principios indicados eran ciertamente novedosos.

III. El modelo alemán de auto-regulación.

10. Mientras que hasta 1984, la ley alemana era el único elemento diferenciador en el panorama europeo de leyes sobre protección de datos, en la actualidad muchas de sus características están presentes en lo que podría denominarse la segunda generación de leyes sobre la materia.

Conviene, por lo tanto, detenernos brevemente en el estudio de la ley alemana para analizar después su influencia parcial en las leyes aprobadas en Finlandia, Irlanda y más recientemente en Holanda.

11. El aspecto principal de la ley alemana es el permitir el procesamiento de datos personales si el derecho lo permite o si el particular ha dado su consentimiento. A diferencia, por lo tanto, de lo que ocurre en otros países donde,

como hemos visto, el tratamiento de los datos únicamente resulta legal cuando se realiza bajo la supervisión de una autoridad central. Paralelamente, en la legislación alemana:

-el sujeto afectado debe estar informado del contenido de un fichero en el que por primera vez se haya almacenado información relativa a el mismo,

-se le concede el derecho de acceso previo pago de una cantidad que no debe exceder los costes directamente atribuibles al suministro de la información,

-los datos erróneos deben ser corregidos,

-es obligatoria la cancelación de los datos inexactos, así como de aquellos que ya no serán utilizados para el objetivo inicialmente previsto,

-los datos personales deben quedar protegidos por adecuadas medidas de seguridad.

12. A la vista de lo expuesto, cabe preguntarse porqué la ley alemana debe entenderse como un sistema de auto-regulación. Básicamente, por la inexistencia de un registro central.

A ello hay que añadir la exigencia de que cualquier compañía que configure un banco de datos de cierta importancia debe designar un Controlador de Datos de la propia compañía. Éste, que actuará como un órgano independiente, puede ser tanto un empleado de la compañía como un consultor o un abogado ajeno a la misma. En cualquier caso, no se le exige que se dedique en exclusiva a esta actividad. La única limitación que impone la ley es que su figura no llegue a plantear conflictos de intereses en la empresa, de modo que, por ejemplo, no podrá desempeñar esta función el Jefe de ventas de un empresa de marketing directo.

IV. Las razones de la actual prevalencia del modelo alemán.

13. Desde mi punto de vista tres razones permiten explicar el progresivo acercamiento durante los últimos años al modelo alemán.

a) *El rápido crecimiento de los micro-ordenadores*

14. Tal y como ha sido señalado previamente, el hecho que determinó la aparición de las primeras leyes de protección de datos fue el peligro de un almacenamiento anómalo de datos en grandes ordenadores centrales. De hecho, se entendía que una máquina que costaba millones de pesetas únicamente podría estar en posesión, y por tanto, ser utilizada por un número reducido de empresas. De ahí que el establecimiento de un sistema de registro centralizado resultara una medida idónea, incluso cuando empresas de tipo medio empezaron a trabajar con ordenadores.

Sin embargo, la proliferación de los micro-ordenadores durante los años 80 ha determinado que prácticamente todas las empresas, e incluso los particulares, puedan configurar su propio banco de datos, de modo que la eficacia de las legislaciones que fundamentan la protección de la intimidad en torno a un registro centralizado ha quedado mermada sensiblemente.

b) *Límites prácticos a la aplicación de la normativa inspirada en el modelo sueco*

15. En la actualidad nadie duda de la validez de los principios establecidos por las Directrices de la OCDE y por la Convención del Consejo de Europa. Con todo, la situación recién descrita ha planteado una importante cuestión, de carácter práctico. ¿Cómo puede la autoridad nacional de protección de datos percatarse de la existencia de pequeñas bases de datos, capaces, de infringir los principios reconocidos internacionalmente?

Supongamos una administración de fincas que elabora un listado de arrendatarios morosos, o un ambulatorio que confecciona una relación de pacientes adictos al alcohol, o una asociación patronal que recoge los nombres de los principales activistas sindicales del sector. Supongamos asimismo que estas pequeñas empresas ponen a la venta sus listados o, incluso, que ellas mismas los utilizan para impedir, vg., la contratación entre las sociedades agrupadas en la asociación patronal de los activistas incluidos en la lista.

En tales casos, las autoridades nacionales de protección de datos presentes en las leyes de protección de datos inspiradas en el modelo sueco únicamente podrán intervenir una vez hayan recibido la queja por parte del particular, esto es, cuando éste se haya visto ya directamente perjudicado.

c) *El movimiento internacional de datos*

16. Las tendencias en la regulación del movimiento internacional de datos han variado sustancialmente desde la adopción de la Ley sueca de protección de datos. En un principio, se consideraba que los datos objeto de

exportación debían ser férreamente controlados, entre otras cosas, porque el procesamiento de datos personales fuera de las fronteras nacionales podría llegar a minar el nivel de protección ofrecido por la ley interna.

Las autoridades de protección de datos de Suecia, Noruega y Austria han tratado por todos los medios de limitar los potenciales daños que podría causar a sus nacionales la exportación de algunos de sus datos personales. En general, los criterios para decidir la permisión o la prohibición de la exportación de los datos eran los siguientes:

-¿Cuál es el país de recepción de los datos? ¿Ha firmado y ratificado la Convención del Consejo de Europa?

-¿Cuál es la organización destinataria y cuáles son sus sistemas de seguridad, por ejemplo?

-¿Qué nivel de sensibilidad presentan los datos a exportar?

17. Por otra parte, las diferentes legislaciones nacionales han establecido diversas soluciones al respecto. De una parte, encontramos el "sistema de licencia formal" a toda exportación de datos, recogido por Suecia y Austria. De otra, el "sistema de notificación", característico de la legislación noruega, por el que se obliga a informar a la Autoridad de Protección de los datos de toda actividad de exportación. El sistema más flexible es el presente en las leyes francesa y británica, consistente en el deber de notificar la voluntad de exportar los datos a través de un formulario en el que se recogen otras cuestiones. Finalmente, la ley alemana carece incluso de mecanismos de control en este sentido, lo que no obsta a que los principios que informan la ley continuen vigentes, de forma que los particulares afectados mantienen sus derechos de acceso y de corrección incluso cuando sus datos estén recogidos en ficheros ubicados en el exterior.

Por lo demás, la práctica noruega de prohibir toda exportación de datos relacionados con información crediticia, ha abierto una nueva orientación destinada a proteger con mayor rigor los datos más sensibles. A veces, se ha tratado de solventar esta cuestión mediante la supresión de determinada información (el nombre, por ejemplo). Esta práctica, que se ha revelado útil respecto de determinadas actividades - la investigación médica, vg. - es, sin embargo, enormemente perjudicial para el sector del marketing directo.

Por último, conviene señalar que la prohibición presente en la ley sueca de exportar a un país que no sea parte en el Convenio del Consejo de Europa

cualquier tipo de datos personales cede si el particular afectado da su consentimiento. La cuestión del consentimiento, pues, resulta capital, por cuanto puede dar a las empresas de marketing directo o a las sociedades bancarias la llave para proceder a una exportación que, en principio, dada la naturaleza de los datos o el país de recepción, era ilegal.

Análisis comparado de las Legislaciones sobre Protección de Datos de los Estados Miembros de la Comunidad Europea

MARIA LAZPITA GURTUBAY
Derecho Público y Ciencias Histórico-Jurídicas.
Facultad de Derecho Universidad Autònoma de Barcelona

SUMARIO

INTRODUCCION

1 - SITUACION ACTUAL DE LA PROTECCION DE DATOS EN LOS ESTADOS MIEMBROS DE LA COMUNIDAD EUROPEA.

1.1- PROTECCION CONSTITUCIONAL.

1.2- LEYES DE PROTECCION DE DATOS EN LOS ESTADOS MIEMBROS DE LA C. E.

2 - ANALISIS COMPARADO DE LAS LEYES DE PROTECCION DE DATOS DE LOS ESTADOS MIEMBROS DE LA COMUNIDAD EUROPEA CON REFERENCIA AL CONVENIO 108.

2.1- PRECISIONES TERMINOLOGICAS.

2.2- AMBITO DE APLICACION.

2.3- REGISTRO Y AUTORIZACION DE LOS SISTEMAS DE INFORMACION.

CONCLUSIONES

BIBLIOGRAFIA

Introducción.

La falta de armonización legislativa en materia de protección de datos es un factor distorsionante en la construcción del Mercado Unico Europeo. Si los derechos fundamentales de los ciudadanos, en particular el derecho a la intimidad, no se garantizan a nivel comunitario, puede verse entorpecido el intercambio transfronterizo de datos, que se ha hecho indispensable para las actividades de las empresas y de los organismos de investigación y para la colaboración entre las Administraciones de los Estados miembros en el marco del espacio sin fronteras. Tal carencia, conlleva el riesgo del traslado del tratamiento informático de los datos de carácter personal hacia el territorio de aquellos Estados miembros con ausencia total de reglamentación o con una regulación menos exigente en la materia, o por el contrario, la marginación de empresas de estos mismos Estados por parte de agentes económicos ubicados en otros estados más escrupulosos, ante el temor de verse envueltos en situaciones escandalosas o irregulares.

Ante esta realidad, resulta preocupante el hecho de que, en el ámbito de la protección de datos, los paises comunitarios no han conseguido aún armonizar satisfactoriamente sus ordenamientos internos. En este momento, la situación se caracteriza por la inexistencia de leyes en algunos Estados Miembros y entre los que se han dotado de legislación interna en la materia, sus sistemas, aunque persiguen los mismos objetivos, son dispares. La mayoría de los Estados miembros están de acuerdo en la necesidad de conciliar la libre circulación de datos con la protección del derecho a la intimidad; sin embargo, la materialización legislativa difiere considerablemente según los paises. Estas diferencias han provocado una situación insatisfactoria por la coexistencia de normas y prácticas administrativas muy diversas dentro de la Comunidad.

El *"Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal"* del Consejo de Europa[1] es el único instrumento internacional jurídicamente vinculante en materia de protección de datos, que, además, ha sido firmado por todos los estados miembros de la CE. Por lo tanto, las instituciones comunitarias deberán tener presente en la versión final de la Directiva sobre protección de datos actualmente en fase de elaboración[2].

1 - Situación Actual de la Protección de Datos en los Estados Miembros de la Comunidad Europea.

En las disposiciones sobre protección de datos se observa, según los Estados miembros, un rango jerárquico y ámbito de aplicación diferente, que, por lo demás, no son mutuamente excluyentes, de forma que pueden coincidir en un mismo Estado. Algunos paises recogen en sus constituciones el derecho

	CONVENIO 108 Firmado	CONVENIO 108 Ratificado	PROTECCION CONSTITUCIONAL	LEYES DE PROTECCION DE DATOS
				En vigor
ALEMANIA	X	X	X*	X
BELGICA	X			X
DINAMARCA	X	X		X
ESPAÑA	X	X	X	X
FRANCIA	X	X		X
GRECIA	X			
IRLANDA	X	X		X
ITALIA	X			
LUXEMBURGO	X	X		X
PAISES BAJOS	X		X	X
PORTUGAL	X		X	X
REINO UNIDO	X	X		X

**Sentencia del Tribunal Constitucional.*

FIGURA 1. PANORAMA LEGISLATIVO EN PROTECCION DE DATOS PAISES MIEMBROS DE LA CE

- 1 Convenio 108 aprobado en Estrasburgo, el 28 de enero de 1981.
- 2 En este sentido se debe matizar, que la Resolución del Parlamento Europeo de 1979 prestaba su apoyo a los trabajos entonces en curso en el Consejo de Europa. Esta actitud favorable hacia el esfuerzo del Consejo continuó posteriormente. Así, en julio de 1981, una Recomendación de la Comisión de la CE invitaba a los Estados comunitarios a que se adhiriesen al Convenio 108, al igual que en la Resolución del Parlamento de 1982. Actualmente el Consejo CE, estudia el Proyecto de adhesión al Convenio 108 por parte de los gobiernos de los Estados Comunitarios, en base al artículo 230 del Tratado de Roma que prevé expresamente la cooperación adecuada de la CE con el Consejo de Europa.

individual a la protección de los datos personales. Otros disfrutan de disposiciones con rango de ley. Una tercera clase de disposiciones está constituida por las que tienen un rango infralegal, derivadas de distintos tipos de acuerdos, por ejemplo, de convenios colectivos o códigos de conducta[3]

Aunque todos los paises miembros de la CE han firmado el Convenio 108, éste debe quedar reflejado en el ordenamiento interno de cada estado miembro. Tres estados poseen específico tratamiento constitucional de la protección de datos personales, y un cuarto, Alemania, goza de reconocimiento pleno del derecho a tal protección por parte de su Tribunal Constitucional. Las normativas con rango de ley, hasta este momento, se encuentran en plena vigencia en diez paises miembros, de los que dos han modificado sustancialmente sus normas, al menos una vez, desde que originalmente las diseñaron, bien para adaptarse a la nueva realidad tecnológica, bien para cumplir con los estándares de protección del Convenio 108.

1.1. - PROTECCION CONSTITUCIONAL.

Algunos paises han incorporado la noción misma de protección de datos en su catálogo de derechos y libertades fundamentales. El primer estado, actualmente miembro de la Comunidad Europea que incluyó este tema en su Constitución fue Portugal en 1976[4]. El texto constitucional dedica íntegramente su artículo 35 a reglamentar la utilización de la informática. Dicho artículo contiene tres párrafos. En el primero se reconoce a todos los ciudadanos el derecho al acceso a todas las informaciones que les conciernen contenidas en registros y el conocimiento del uso a que se destinan. El segundo establece que la informática no debe servir para el procesamiento de datos relativos a convicciones políticas, creencias religiosas o vida privada, salvo cuando se refiera al tratamiento con fines estadísticos de datos no identificables. El tercer párrafo contiene una prohibición de atribuir a los ciudadanos un número nacional único. En este último párrafo se refleja un cierto "principio de desconfianza" dirigida a prevenir las posibles interconexiones de datos, a pesar de todas las garantías legales[5].

En 1978, la Constitución española incluyó, en la sección primera del Capítulo segundo del título primero referida a los derechos fundamentales y las libertades públicas, aunque más parco y ambiguo que el portugués, una pro-

- 3 GARZON CLARIANA, G. *Informatización de la sociedad y derecho de gentes.*, Cursos de derecho internacional de Vitoria-Gasteiz, 1983, p. 118.
- 4 Constitución de la República Portuguesa, aprobada por la Asamblea Constituyente en sesión de 2 de abril de 1976. Edición oficial, Impresa Nacional, Casa de Moneda, Lisboa, 1976.
- 5 MARCELO, J.: *Libertades e informática en Europa. Parte I: Antecedentes.* NOVATICA nº 94, p. 68.

tección específica de la intimidad frente a la informática. El artículo 18. 4, establece textualmente *"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"*[6]. El mimetismo del legislador español en la redacción del artículo 18.4 con la constitución portuguesa se ciñó a la preocupación genérica por el uso de la informática: la Carta Magna Lusa es más específica para la protección de datos que la española. El apartado 4 del artículo 18 ha sido estimado por algunos constitucionalistas como superfluo, debido a que ya se enuncia una declaración del reconocimiento general al derecho a la intimidad en el apartado 1 de dicho artículo[7]. Si la parquedad del 18.4, que no aparece aclarado en sus fines ni su alcance, permite discrepar sobre su alcance e importancia, hay práctica unanimidad en calificar tal tutela como claramente insuficiente[8].

Los Paises Bajos. con la reforma efectuada en 1983 de su Carta Magna, elevó al rango constitucional la protección de los datos personales. En la Sección 10, párrafo 2, se establece el mandato de regular por Ley la protección de la intimidad individual en lo concerniente al almacenamiento y revelación de los datos personales. En su párrafo 3, impone regulaciones en relación con los derechos de los individuos a conocer sus propios datos y el uso que se haya hecho de ellos, así como la posibilidad de corrección de tales datos. El mandato constitucional deja también patente la necesidad de legislar este campo específico, que había sido objeto de preocupación social desde que en 1971, se quiso elaborar el censo por ordenador.

El Tribunal Constitucional de Alemania, en su Sentencia sobre el Censo, completó los derechos constitucionales de la personalidad a pesar de la inexistencia en la Ley Fundamental de 1949, por la época en que fue redactada, de un derecho específico sobre el tema; el Tribunal Constitucional, en el caso citado, determinó las condiciones legales para regular la recogida, almacenamiento y procesamiento de datos personales por el Estado. Sobre la base del derecho a la dignidad humana y al libre desarrollo de la personalidad dicho Tribu-

- 6 La Constitución en su artículo 20, reconoce y protege en su párrafo "1º, el derecho a comunicar o recibir libremente información veraz por cualquier medio de difusión, más adelante el párrafo 4º establece *"Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente en el derecho al honor, a la intimidad a la propia imagen y a la protección de la juventud y de la infancia."* Complementariamente con el tema que nos ocupa el artículo 105 b) de la Constitución dice que la Ley regulará el libre acceso de los ciudadanos a los Archivos y Registros, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.
- 7 Romeo cita a O. Alzaga (*Comentario sistemático a la Constitución Española de 1978*). ROMEO CASABONA, C.M.: *Poder informático y seguridad jurídica.* Editorial Fundesco. Madrid, 1986, p. 28.
- 8 Ver MORALES PRATS, F. *La tutela penal de la intimidad: privacy e informática.* Ediciones Destino Barcelona 1984, p. 22. También ver BOIX REIG, J.: *Protección Jurídico penal de la intimidad e informática.* CONGRESO SOBRE DERECHO INFORMATICO, 22-24 de Junio, Zaragoza, 1989, p. 462, y también 459 y ss.

nal garantizó la continuidad de las libertades básicas, consagradas con anterioridad, con la formulación de un nuevo derecho, el derecho a la autodeterminación informativa[9].

A modo de resumen, cabe indicar que la tutela de los datos personales de rango constitucional en el ámbito comunitario es heterogénea. La Carta Magna Lusa resalta la protección de una categoría particular de datos (los llamados datos sensibles) y también la prohibición de interconectar ficheros mediante la prohibición de asignar a los ciudadanos portugueses un número nacional único[10]. La protección española es tan sólo nominal y emplaza al legislador a regular el uso de la informática frente a las amenazas a la esfera privada. La Ley fundamental de Bonn no contiene ninguna referencia literal al derecho a la intimidad, pero la sentencia del Tribunal Constitucional alemán incorpora la autodeterminación informativa al catálogo de derechos de la personalidad. La última aportación de rango constitucional, la de los Paises Bajos, opta por introducir la protección derivada de los principales derechos derivados del Convenio 108 en su carta magna (derecho a conocer, derecho de acceso, derecho de corrección).

1.2. - LEYES DE PROTECCION DE DATOS EXISTENTES EN LOS ESTADOS MIEMBROS DE LA COMUNIDAD EUROPEA.

Las primeras leyes sobre esta materia, conocidas como primera generación de protección de datos, tenían en común la convicción de que había llegado el momento de reaccionar ante la informatización progresiva de la sociedad y también, la incertidumbre acerca de sus implicaciones inmediatas, así como

- 9 Tal derecho está integrado por una serie de facultades, que se reconocen al sujeto activo de la protección de datos, todas ellas relativas a la captación, tratamiento y conservación y a la transmisión de sus datos personales. Denninger afirma que el derecho a la autodeterminación informativa no fue una invención del alto tribunal de Karlsruhe, "*ni de hecho, ni de nombre*"; e incluye esta jurisprudencia particular dentro del derecho general a la personalidad. Para la doctrina alemana, el objeto de protección, parte de la posibilidad de cooperación responsable del individuo en los asuntos de *res publica* incluyendo la facultad de la persona de "*decidir básicamente por sí misma cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida*"; por lo tanto, es el valor y dignidad de la persona que actúa con libre autodeterminación para formar parte de una sociedad libre. DENNINGER, E.: *El derecho a la autodeterminación informativa,* en PEREZ LUÑO, A. E,: *Problemas actuales de la documentación y la información jurídica.* Ed. Tecnos. Madrid, 1987, pp. 268. Ver también PEREZ LUÑO, A. E.: *Nuevas tecnologías, sociedad y derecho.* Fundesco, Madrid, 1987, p. 87, revisado posteriormente en PEREZ LUÑO, A. E., *Los derechos humanos en la sociedad tecnológica,* en LOSANO, M. G.; PEREZ LUÑO, A. E.; GUERRERO MATEUS, Mª F.: *Libertad informática y leyes de protección de datos personales.* Centro de Estudios Constitucionales. Cuadernos y Debates nº 23. Madrid, 1989. p. 152. Por último, MURILLO DE LA CUEVA, P.L.: *El derecho a la autodeterminación informativa,* Tecnos. Madrid, 1990, pp. 149.
- 10 El número nacional único es, sin duda, el elemento clave para lograr una efectiva interconexión de bases de datos, y paises de gran tradición democrática que lo utilizan han sido también pioneros en la protección de datos, como, por ejemplo, Suecia. Ver SIZER, Richard; NEWMAN, Philip. *The Data Protection Act. A Practical Guide.* Gower. Hants, 1986, p. 9-11. También señalan estos autores que si la preocupación por la intimidad en Gran Bretaña apenas tiene tradición y continuidad, los intentos para imponer un número nacional único (el último data de enero de 1984, cuando fracasó un intento de establecer un número nacional único en la seguridad social) se han fustrado en las islas.

de las medidas precisas que debían tomarse[11]. Eran rígidos instrumentos de una época caracterizada por una tecnología hoy casi obsoleta: unos bancos de datos muy caros, escasos, voluminosos y, por lo tanto, fácilmente localizables.

Asi en 1977, la República Federal Alemana, promulgó la Ley Federal sobre Protección de Datos de 27 de enero, que entró en vigor el 1 de enero de 1978, ocho años después de que se aprobara en el *Land* de Hesse, la primera normativa en la materia[12].El primer artículo de la ley federal establece que el objeto de la norma es *"la protección de datos que tiene como fin impedir la lesión de bienes dignos de tutela de las personas interesadas, garantizando los datos relativos a su persona de abusos cometidos con ocasión de su almacenamiento, transmisión, modificación o cancelación (elaboración de datos)"*[13]. Común a todas las leyes tutelares son las previsiones institucionales para la articulación de los órganos a los que se confía la aplicación de la ley. Siguiendo el molde de la ley del *Land* de Hesse, se establece la figura del Comisario para la protección de datos en su doble función de instancia a recurrir y de "perro guardián" de la normativa. La ley alemana diferencia por un lado entre los sectores público y privado, el sector público se divide a su vez en dos niveles el federal y el regional. A nivel regional tiene prioridad la ley de cada *land*, quedando la autoridad del Comisario federal para la protección de datos restringida al nivel federal y a los *landers* en los que no exista ley regional para la protección de datos. La totalidad del sector privado depende de la autoridad supervisora del *Lander*.

En Francia[14], el 6 de enero de 1978, se aprobó la Ley sobre *"Informática, Ficheros y Libertades"*[15]. Hay que destacar el artículo 1 de esta ley, que refleja, la intención del entramado normativo que se desarrolla a continuación: *"La informática deberá estar al servicio de cada ciudadano. Su desarrollo deberá tener lugar dentro del marco internacional. No deberá atentar la identidad humana ni a los derechos del hombre ni a la vida privada ni a las libertades individuales o públicas"*. La intención de esta ley es más amplia que otras normas y se propone abarcar múltiples aspectos de las nuevas tecnologías de la información.

- 11 Ver SIMITIS, S.: *New Trends in National and International Data Proteciton Law.* en DUMORTIER, J. (Ed.): *Recent developments in data privacy law. ICRI Conference.* Leuven University Press, Lovaina, 1992, p. 17.
- 12 La primera norma europea tutelar de datos fue promulgada en Hesse en 1970, su breve articulado preveía la regulación del acceso a la información de los bancos de datos públicos y la supervisión de su funcionamiento a un *ombudsman* especializado, el Comisario para la protección de datos.
- 13 Ver Informática. *Leyes de Protección de datos.* Núm. 3. Servicio Central de Publicaciones. Madrid. 1983, p. 35-36.
- 14 En Francia, se creó en el año 1974 la Comisión "Informática y Libertades" con la finalidad de proponer al Gobierno "medidas tendentes a garantizar que el desarrollo de la Informática en el sector público, semipúblico y privado se realizará en el respeto a la vida privada, a las libertades individuales y a las libertades públicas". CARRASCOSA LOPEZ, Valentín: *Derecho a la intimidad e informática.* En Informática y Derecho, nº 1, 1992, p. 19
- 15 Loi relative a l' Informatique, aux fichiers et aux libertes, nº 78-17 de 6 de enero de 1978, J.O. 227, de 7 de enero de 1978. Dicha Ley entró en vigor para el sector público el 1 de noviembre de 1979, y para el sector privado el 1 de enero de 1980. Ver Informática. *Leyes de Protección de datos.* Núm. 3. Servicio Central de Publicaciones. Madrid. 1983, p. 35-36.

La Ley francesa opta por un órgano colegiado, la Comisión Nacional de la Informática y las Libertades (CNIL), compuesto de diecisiete miembros elegidos por diferentes instituciones públicas. Es un autoridad administrativa independiente que posee amplias potestades reglamentarias, de control y sancionadoras, y sus decisiones son apelables ante el Consejo de Estado. Tres subcomisiones se han formado en el seno del CNIL que se han especializado en unos usos particulares del procesamiento automatizado de datos: de informática y relaciones laborales, de informática y la investigación científica, y la de informática y libertad de expresión.

En Dinamarca, la ley de protección de datos se promulgó en 1978 articulando dos normativas, una concerniente al sector público (conocida como *PARA*) y otra al sector privado (denominada, *PRA*).

El Gran Ducado de Luxemburgo aprobó, en marzo de 1979, una ley reguladora del uso de los datos personales procesados automáticamente. La aplicación de la Ley es supervisada por el Ministro de Justicia, quien es requerido, en ciertos casos, para oir la opinión de un Comité Consultivo de abogados y expertos en informática nombrados por el Gran Duque.

El "*Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal*", del Consejo de Europa de 1981, marca el inicio de una segunda etapa en la historia de la protección de datos[16]. El Convenio no fue innovador, reflejando los puntos de vista ya recogidos en la leyes existentes, la gran aportación fue que los principios de protección de datos fueron investidos con la autoridad de un organismo internacional, lo que propició la expansión de las leyes de protección de datos, conocidas como de segunda generación y la revisión de las leyes anteriores, para adecuarse a la nueva realidad tecnológica[17] y al Convenio del Consejo de Europa.

- 16 La OCDE aprobó el 23 de septiembre de 1980 la "*Recomendación relativa a las directrices aplicables a la protección de la vida privada y a los flujos transfronterizos de datos personales*". que han favorecido la consagración de los principios jurídicos sobre protección de datos enunciados en el Convenio del Consejo de Europa, entonces en fase de realización. GARZON CLARIANA, G. *Informatización de la sociedad y derecho de gentes*, Cursos de derecho internacional de Vitoria-Gasteiz, 1983, p. pg. 125.
- 17 Además del refinamiento en *hardware* y *software* en todas las plataformas, la aparición de nuevas aplicaciones, el abaratamiento de los soportes físicos y la extensión cuasi universal del microordenador, hay tres fenómenos que han sido identificados por la doctrina en lo relativo a las leyes de protección de datos. En primer lugar, la trivialización del procesamiento de datos, causada por la evolución de los grandes sistemas informáticos de los años sesenta, escasos y poco accesibles, a los numerosos microordenadores personales interconectados en redes de área local muy potentes y accesibles. En segundo lugar, la diversificación de los datos: las clásicas bases de datos de grandes organizaciones no son hoy en día los únicos sistemas de información existentes; existen también sistemas expertos, sistemas de microficha, discos ópticos con y sin imágenes y bases de datos en CD-ROM. Por último, el creciente sistema de distribución e información interactivos tales como sistemas bidireccionales de televisión por cable, servicios educativos, juegos interactivos, sistemas expertos y correo y conferencias electrónicas. BING, J.: "*Impact of...*" *op. cit.* p. 3 y ss.

Dinamarca reformó las normativas en dos ocasiones: la primera en 1987, ampliando el derecho de acceso de los sujetos de los datos[18] y, más adelante, en 1991, se simplificó el control de los ficheros públicos.

En Alemania, la Ley federal fue reformada en 1990, las enmiendas entraron en vigor el 1 de junio de 1991[19]. Amplía considerablemente su ámbito de aplicación en el sector público, permitiendo desde la tutela de nuevos soportes de información digital (imágenes y sonidos) hasta disposiciones reguladoras de la recogida de datos.

Luxemburgo ha postpuesto las reformas en curso hasta que se apruebe la Directiva de la Comunidad Europea en la materia[20].

El sistema francés es el más flexible de los vigentes en Europa. La actuación del CNIL regulando nuevas áreas o implementando los acuerdos convencionales mediante reglamentos ha conformado un estilo de constante innovación normativa[21].

El gobierno británico había sido reacio a establecer restricción legal alguna al procesamiento de datos no promulgando su *Data Protection Act* hasta 1984[22]. Hay que resaltar, que la temprana sensibilidad del Parlamento[23] ante los acosos de la intimidad por la informática no lograba ser plasmada en una normativa, y fue la aprobación del Convenio decisiva para reactivar el proceso legislador, ante el temor de que en lo sucesivo las compañías extranjeras no procesaran sus datos personales en Gran Bretaña.

La tarea de garantizar el cumplimiento de la ley recae en dos órganos, el *Registrar* quien debe llevar el registro y control de los bancos de datos persona-

- 18 Las nuevas Leyes entraron en vigor el 1 de abril de 1988. Ver CAMERON, Euan & BLUME, Peter: *Data Protection Law in the United Kingdom and Denmark,* University of Leicester, Leicester, 1988, pg.15. El ámbito de aplicación de la Ley ha sido ampliado y aumentando sensiblemente el numero de Instituciones que se ven afectadas por la misma. PEERS, Eddy; BUCKLEY, Bill. *Computers and Data Protection.* Deloitte, Haskins & Sells. London. 1988. pg.48.
- 19 Ver *TDR Report,* Nov-Dec 1991, pp. 25-27. También en *Privacy Law & Business.* Dec 1991, pp 4-5.
- 20 *Data Protection Roundup.* PRIVACY LAWS & BUSINESS. July 1991, pp 2 y ss.
- 21 Por ejemplo, el CNIL, sensible a las implicaciones sociales del problema del SIDA, ha establecido que así un paciente seropositivo debe autorizar previamente por escrito la informatización de sus datos. Ver FAUVET, Jacques: *Diez años de aplicación del Convenio Europeo de Protección de Datos.* Novática, núm. 96, p. 14.
- 22 La Ley entró en vigor el 12 de julio de 1984, pero sus principales disposiciones sobre el registro no tuvieron efecto hasta el 11 de mayo de 1986.
- 23 Dos comités informaron al Parlamento de la protección que la *common law* brindaba a los británicos ante la informática, además de las posibles iniciativas legisladoras que podrían tomarse: Younger (1972) y Lindopp (1976). Ver LOSANO, Mario G. *Los orígenes del "Data Protection Act" inglesa de 1984.* en LOSANO, Mario G.; PEREZ LUÑO, A. E.; GUERRERO MATEUS, Mª F.: *Libertad informática y leyes de protección* ... op. cit., 9-60. Ver también, CHALTON, S. N. L. y GASKILL, S. J.: *Enciclopedia of Data Protection.* Sweet & Maxwelll, Londres, 1989, pp. 1002 y ss.

les, emitir líneas directrices de comportamiento y recibir las quejas; y el *Data Protection Tribunal*, compuesto por 31 miembros que es la instancia de apelación de las decisiones del *Registrar*[24].

La ley irlandesa de 1988 muy similar a la británica sigue fielmente el modelo del Convenio del Consejo de Europa. El "*Irish Data Protection Commissioner*" es la autoridad encargada de velar por el funcionamiento de la norma tutelar. Entre los poderes de dicha autoridad está el conceder permiso de exportación de datos personales[25].

Cuando en los Paises Bajos, en 1971, se intentó procesar el censo por ordenador, se organizó una polémica en torno a la violación de la intimidad, que supuso la creación de un Comité Estatal para la Protección de la Intimidad. La tutela legislativa de la intimidad informática se inició con la enmienda de 1983 a la Constitución que preveía la creación de un cuerpo normativo al efecto. Tras un agitado periplo en la Cámara Alta y con varios meses de retraso, se publicó la ley sobre ficheros de datos personales (*Wet Persoonregistraties*) en enero de 1989. La ley pretende cumplir el mandato constitucional de articulación de una norma de protección de la intimidad con respecto al procesamiento de datos personales, la implementación del Convenio del Consejo de Europa y, por último, intenta proteger la competitividad de la industria nacional de las tecnologías de la información[26]. Se establece una Cámara de Registro que vela por el cumplimiento de las normas y por la tarea de establecer los códigos de conducta, cumple el deber de informar a las autoridades de las implicaciones prácticas de la ley y, como en otras leyes, atiende las reclamaciones pertinentes.

La ley portuguesa de protección de datos[27], que entró en vigor en mayo de 1991, ampliando la tutela establecida por la Constitución de 1976, consagra los principios convencionales del Consejo de Europa. La Comisión Nacional para la Protección de Datos Personales Automatizados, órgano encargado de velar la aplicación de la ley, está compuesta por siete miembros, tres de los cuales son elegidos por el Parlamento, dos por las instancias judiciales y dos por el Gobierno. La protección normativa es exhaustiva en lo relativo a la tute-

- 24 V. NIBLETT, Brian, *Data Protection Act*, Longman, London, 1984,; CAMERON Euan & BLUME Peter, *Data Protection Law in the United Kingdom and Denmark*, University of Leicester, Leicester, 1988. NCC & DTI, *Security and 1984 Data Protection Act*, NCC Publications, London, 1987, GULLEFORD, Kenneth. *Data Protection in Practice*. Butterworths. London. 1986. SIZER, Richard; NEWMAN, Philip. *The Data Protection Act. A Practical Guide*. Gower. Hants. 1986.
- 25 Ver CLARK, Robert; LINEHAM; Donald C.;. 1989. *Data Protection Law in Ireland*. The Round Hall Press. Dublin. 182
- 26 Ver A. NUTGER, *op. cit. pp.* 145-48.
- 27 *Lei da Protecçao de Dados Pessoais face à Informática* Lei Nº 10/91. DIARIO DA REPUBLICA. Número 98, Serie I - A de 29 de abril de 1991, pp. 2366-2372.

la de los datos sensibles, la interconexión de ficheros y los flujos internacionales de datos personales.

España, además del ya comentado emplazamiento constitucional del artículo 18, párrafo 4, contrajo otros compromisos posteriores, de carácter internacional; como la obligación contemplada en el artículo 4 de la Convenio 108 del Consejo de Europa[28] y el compromiso adoptado por el Gobierno español con la firma del protocolo adicional del Convenio de 1990 en aplicación del acuerdo de Schengen de 1985, que redoblaban la necesidad de disponer de una ley orgánica en tutela informática. Con varios años de retraso sobre lo esperado, el 31 de octubre de 1992 se publicaba en el BOE la *Ley Orgánica para la Regulación del Tratamiento de Datos de Carácter Personal* (L. O. 5/1992) , que entró en vigor el 31 de enero de 1993. No obstante, ha sido recibida con importantes reservas. siendo objeto de varios recursos y cuestiones de incostitucionalidad, aun no resueltos por el Tribunal Constitucional.

La orientación general de la Ley Orgánica es, en gran parte, similar a las leyes de la segunda generación. En la segunda parte, se configura la autoridad de control, la Agencia para la Protección de Datos, una entidad de Derecho Público, a cuyo frente se sitúa un Director quién ejerce sus funciones de modo independiente[29].

En Bélgica desde 1976,se han presentado numerosos proyectos, no siendo aprobada la ley general en tutela de datos personales hasta el 8 de diciembre de 1992[30]. En 1983, se creó el Registro Nacional de Personas Físicas y en 1982 la Comisión Consultiva para la Protección de la Vida Privada.

Dos estados miembros Italia y Grecia a pesar de haber firmado el Convenio 108 no han aprobado todavía su correspondiente ley de protección de datos. La república italiana ha vivido varios procesos de impulso legislativo que no han dado fruto alguno[31]. En Grecia los pocos proyectos presentados no han prosperado debido a las sucesivas citas electorales.

- 28 Ratificado por España el 27 de enero de 1984. Publicado en el BOE nº 274 de 15 de noviembre de 1985.
- 29 Se contempla, sin embargo, la obligación de elevar un informe anual al Ministerio de Justicia (artículo 36.k).
- 30 No obstante, Bélgica adoptó algunas regulaciones sectoriales relativas a funcionarios públicos (1982), al censo (1983), al crédito (1985) y a la seguridad social (1990). Ver BERKVENS, Jan: *Belgian Data Protection Reviewed.* TDR, Nov-Dec 1991.
- 31 El último, presentado en 1989, por un Comite dirigido por el profesor Mirabelli, era una revisión del anterior proyecto: *Constituzione de esercizio delle bancche di dati personall ad elaborazzione informatica.* Disegno de Legge. Camara del Deputati. N.1657, 5 mayo 1984., rechazado en 1985.

2 - Análisis Comparado de las Leyes de Protección de Datos de los Estados Miembros de la Comunidad Europea con Referencia al Convenio 108.

Como se ha indicado previamente, el texto convencional del Consejo de Europa contribuyó decisivamente a acelerar la promulgación de normas tutelares y a reformar las existentes. El efecto esperado de una ratificación general era lograr un mínimo nivel equivalente de protección entre las distintas partes contratantes[32], dando como resultado, por un lado, que las personas de los Estados signatarios disfrutaran de los mismos derechos básicos sin tener importancia el lugar donde sus datos personales fueran procesados y por otro, que los datos pudieran circular libremente entre los paises que hayan puesto en vigor los principios fundamentales del Convenio[33].

Dichos principios, también denominados su *núcleo irreductible*, presentan la doble cualidad de constituirse como bases y como mínimos[34]. La primera cualidad se deduce del artículo 4, donde se establece que todos los Estados contratantes tienen la obligación de adoptar en su derecho interno las medidas necesarias para el cumplimiento de dichos principios[35]. El segundo aspecto, el constituirse como mínimos se desprende del artículo 11, que permite a los estados signatarios *"establecer una protección más amplia"* que la prevista en el Convenio.

Aunque todas las leyes internas siguen el modelo del Convenio, la protección ofrecida en la práctica varía sensiblemente de unos paises a otros. El Convenio es enunciado en términos muy generales. Los principios básicos de protección hacen referencia a la calidad y seguridad de los datos, a las garantías de las personas cuyos datos han sido registrados, al régimen especial a que someter los datos que merecen una protección cualificada y a las excepciones y restricciones legítimas.

- 32 En el número 20 del *Explanatory Report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series, No.108. Council of Europe. Strasbourg, 1981. De aquí en adelante se citará como la Memoria Explicativa.
- 33 El Convenio 108 regula los FID en el artículo 12, cuyo objetivo es el de conciliar las exigencias de la protección eficaz de los datos personales con el principio de libre circulación de información, independientemente de la existencia de fronteras, consagrado en el artículo 10 del Convenio Europeo de los derechos del hombre. En relación con el artículo 12, se indica en la Memoria Explicativa núm. 67: *"la razón de esta norma estriba que todos los estados contratantes, por haber suscrito el núcleo irreductible de las normas de protección de datos contenido en el capítulo II, ofrecer un cierto nivel mínimo de protección."*
- 34 GARZON CLARIANA, G.: *La protección de los datos personales ... op. cit.*, p. 17.
- 35 El artículo 10 lo completa *"Cada parte se obliga a prever las oportunas sanciones y recursos para los casos de violación de las disposiciones del Derecho interno que dieren cumplimiento a los principios fundamentales de protección de datos enunciados en el presente capítulo."*

Todas las leyes recogen de modo parejo la enunciación convencional de estos principios, pero el Convenio indica muy vagamente las medidas que los estados contratantes deben adoptar para que tales principios sean operativos en la práctica. La armonización de las leyes podría alcanzarse en cuanto a la formulación de los principios. Es en cuestiones como las relativas a la organización del sector público, las competencias de los órganos públicos y los procedimientos de la administración pública donde prevalecen las tradiciones y los prejuicios nacionales[36].

Dada la coexistencia de normas y prácticas administrativas muy diversas dentro de la comunidad, las normas tutelares se han desarrollado con terminologías no siempre coincidentes; el ámbito de aplicación difiere de unas leyes a otras y se articulan reglas sustantivas en el tratamiento informático que contienen matices y variaciones apreciables. Seguídamente se analizan algunas cuestiones determinantes para ver cúal es la implantación real del Convenio como solución armonizadora en el ámbito comunitario de protección de datos

2.1. - PRECISIONES TERMINOLOGICAS.

El término **datos**, no explicitado por el Convenio 108, es únicamente definido por las leyes de Irlanda y Reino Unido. Ambas leyes lo hacen de forma diferente siendo la definición británica más restringida que la irlandesa, *"Data"* es definido en el Reino Unido como *"toda información, registrada de manera, que pueda ser procesada por un equipo que opere automáticamente en respuesta a las instrucciones que se le hayan dado para dicho propósito"*. El hecho de incluir la palabra registrada (*recorded*) limita el alcance de la definición. La ley irlandesa habla de *"La información que pueda ser procesada"* y abre el alcance de la ley a nuevas aplicaciones tecnológicas.

El término **datos personales**, definido en el Convenio como: *"toda información concerniente a una persona física identificada o identificable"*[37], es muy homogénea en todas las normas, consensuando la definición al uso de los textos internacionales. La ley francesa considera como "datos personales" las informaciones que permitan directa o indirectamente la identificación de los titulares de las informaciones. La ley española los define en los mismos términos que el Convenio; de manera similar lo hacen Alemania, Dinamarca,

■ 36 SELMER, K: *Data Protection Policy.*, en SEIPEL, P.: *From Data Protection to Knowledge Machines.* Kluwer, Computer Law Series/5. Deventer 1990, p.12.

■ 37 El término "*Datos Personales*", esta definido en el artículo 2 a) del Convenio. La Memoria Explicativa núm. 28 matiza; " *por persona identificable se entiende una persona que puede fácilmente ser identificada, no se incluye al respecto la identificación de personas por métodos complejos.*"

Luxemburgo, Bélgica, Paises Bajos y Portugal. Los dos últimos indican expresamente que la identificación no debe suponer una desproporcionada cantidad de dinero y tiempo. La ley de Luxemburgo amplía la consideración de datos personales a datos identificables referentes a la familia o a la comunidad en su conjunto. El Reino Unido los define como la información relativa a un individuo que pueda ser identificado a partir de dicha información o de tal información cruzada con otra que posea el responsable del proceso informático, incluyendo cualquier opinión sobre el individuo y excluyendo las valoraciones de dicho responsable con respecto al individuo[38].

El Convenio utiliza el término **responsable del fichero**, para describir a la persona física o jurídica, autoridad pública, servicio u organismo competente para decidir sobre qué clases de datos de carácter personal deben ser almacenados y qué operaciones deberán serles aplicadas. En Alemania el término utilizado es *"unidad de almacenamiento"* haciendo hincapié en cualquiera *"que almacene datos por cuenta propia o posea datos almacenados por otros"*, contenido casi idéntico al termino *"data user"* de la ley británica. La ley española se expresa en los mismos términos que el Convenio, y del mismo modo lo hacen la ley francesa y la belga (*maitre du fichier*) la irlandesa (*data controller*), la neerlandesa (*controller of the file*). La ley danesa PRA define de modo más restringido al *"owner of the register"* en términos de empresa. La ley de Luxemburgo es la que establece un término más amplio, añadiendo normas sobre los responsables de fichero que acceden a datos personales sitos fuera del Ducado[39].

2.2. AMBITO DE APLICACION.

El Convenio del Consejo de Europa en principio aplicable a los datos de las personas físicas que sean objeto de tratamiento automatizado[40](art. 3.1), permite a las partes contratantes, por un lado, extender la aplicación de sus

- 38 El Lindop Committee consideró que el termino "*information*" se refería al resultado final de la elaboración, mientras que el termino "*data*" denominaría la informaciones iniciales a partir de las cuales se realizan todas las operaciones sucesivas. El Informe del citado Comité, consideró como "*Personal Information*", "*toda información que se refiere a cualquier dato del sujeto, que es o puede ser identificado por medio de informaciones como el nombre, la dirección, la edad de nacimiento o el numero telefónico*". LOSANO, M.G.: *El origen del "Data Protection Act" inglesa de 1984* en LOSANO, Mario G.; PEREZ LUÑO, A. E.; GUERRERO MATEUS, Mª F. *op. cit.* pg. 47.
- 39 El Convenio del Consejo de Europa articula dos definiciones más: fichero automatizado y tratamiento automatizado, definiciones de un momento tecnológico superado. Las Conferencias de Comisarios de Protección de datos han criticado repetidamente la obsolescencia en que ha caído la terminología como fichero de datos: "*los datos deben protegerse a lo largo de todas las etapas del proceso*". Ver HARREMOES, Erik: *Summary of Conclusions.* XIIIth Conference of Data Protection Commissioners, Strasbourg, 2-4 October 1991. p. 2
- 40 El artículo 2 a) define los datos de carácter personal como los referentes a las personas físicas. El art. 2 c) define fichero automatizado como "las operaciones siguientes efectuadas en todo o en parte con ayuda de medios automatizados: almacenamiento de datos, aplicación de tales datos a operaciones lógicas o aritméticas, o de ambas su modificación, borrado, recuperación o difusión.

leyes internas sobre protección de datos a los ficheros manuales y a las personas jurídicas[41] y, por otro, reconoce a los estados signatarios la facultad de sustraer la aplicación del Convenio a categorías enteras de archivos automatizados (art.3.2).

El panorama de las leyes europeas de protección de datos, referentes al ámbito de aplicación se dibuja en dos planos principales:

a) - Según la naturaleza física de los datos, **ficheros automatizados** o **manuales**. Siendo el objeto que animó el proceso legislativo, la protección de los ficheros automatizados es recogido por todas las leyes, No son aplicables a los ficheros manuales las leyes de Dinamarca (PARA), Irlanda, Luxemburgo, Reino Unido y Portugal. La ley francesa es aplicable por ejemplo, a los datos sensibles como las opiniones políticas y religiosas, almacenados en archivos manuales, así como a la información almacenada en papel por la prensa escrita y la audiovisual. La ley de los Paises Bajos y la danesa (PRA) son aplicables a los ficheros manuales, siempre y cuando pueda accederse a los datos recogidos en dichos ficheros sistemáticamente. Alemania incluye la intención de comunicar a terceras partes como el requisito que permite a la ley proteger ficheros manuales[42]. La ley española, es aplicable a ficheros automatizados y a los manuales en soporte físico susceptible de tratamiento automatizado.

b) Según las personas a las que los datos hacen referencia, es posible distinguir entre datos relativos a las **personas físicas** y a las **personas jurídicas**.

Todas las leyes recogen el supuesto común de que los datos conciernen a personas físicas. En algunos Estados miembros se aplican también a las personas jurídicas: la Ley Luxemburguesa y la Danesa (PRA), extienden su aplicación a las personas jurídicas. En la Ley francesa los derechos de acceso y rectificación pueden ser ejercitados por personas jurídicas[43]. Las Leyes de Irlanda y el Reino Unido son aplicables a *"individuals"*[44]. La normativa de los Paises Bajos también sigue el criterio limitado, pero en los supuestos en los que la ley se refiere a *one-man business* o pequeñas sociedades, puede considerarse como

- 41 Garzón apunta que la protección de los datos relativos a personas jurídicas es un tema polémico; de ahí que el Convenio opte por una solución de compromiso. GARZON CLARIANA, Gregorio: *La protección de los datos personales ... op. cit.*, pg.16 y 17
- 42 GEBHARDT, H.P.. *La protección de datos en paises industrializados. Principios y situación jurídica.* TELOS. 19891, pp 129-140.
- 43 Extensión realizada el de julio de 1984 por una decisión administrativa del CNIL, Autoridad francesa de Protección de datos.
- 44 En los textos ingleses, cuando se habla de *"persons"*, se hace referencia a las personas físicas y jurídicas, el término *"individual"* por el contrario hace referencia solamente a las personas físicas. PEREZ LUÑO, A.E.: *La libertad informática.... op. cit.* pg. 46.

datos personales si ello no supone una complicación o un largo y costoso proceso para relacionar una información con el sujeto de datos.

Hay también que destacar la protección cualificada que ofrece el Convenio a ciertas categorías de datos, por su calificación de sensibles[45]. El Convenio deja al arbitrio de cada derecho interno las garantías apropiadas aplicables al procesamiento de este tipo de datos personales así como los tipos de datos que pueden ser considerados sensibles[46].

Las diferentes restricciones y matizaciones en lo referente al ámbito de aplicación están en parte motivadas por el criterio que se siga a la hora de determinar cómo y qué datos pueden afectar al individuo, siendo también importante la tradición existente en cada país de respeto a la intimidad individual. En relación con el Convenio, lo más grave es la posibilidad que ofrece a los paises ratificantes de excluir categorías enteras de archivos automatizados, lo que significa que dichos datos no están protegidos por las leyes que los han excluido, haciendo necesario conocer el criterio adoptado por cada una de las leyes nacionales para valorar la protección ofrecida en cada situación concreta, resultando particularmente difícil en un contexto internacional[47].El artículo 14 del Convenio, referente a la mutua asistencia, aunque puede proporcionarse cierta ayuda a los afectados, no está concebido para lograr una colaboración interestatal en la materia tendente a aminorar las diferencias entre las leyes de protección de datos.

2. 3. Autorización y Registro de los Sistemas de Información.

El Convenio 108, reconociendo que debe existir un Registro General de bancos de datos[48], deja abierto al criterio de cada país signatario el sistema que deba adoptarse para la autorización, creación y registro de ficheros. En varios Estados Miembros, la creación de un fichero está sujeto a la previa autorización de la agencia nacional sobre protección de datos. Las leyes europeas

- 45 Artículo 6: "*Los datos de carácter personal que revelaren el origen racial, las opiniones políticas, las conviciones religiosas u otras convicciones, asi como los datos de carácter personal relativos a la salud o a la vida sexual, no podran ser elaborados automáticamente a menos que el Derecho interno previere las oportunas garantías. La misma regla se aplicara a los datos de carácter personal referentes a condenas criminales.*".
- 46 Por ejemplo Francia y Portugal añaden la filiación sindical en la lista de datos sensibles.
- 47 Ha sido, precisamente, la excepción para los ficheros de las Administraciones Públicas de la garantía de informar al afectado, objeto de recurso de inconstitucionalidad por parte del Defensor del Pueblo.
- 48 El apartado b) del artículo 5 del Convenio 108: "*Registrados para unos fines determinados y legítimos y no utilizados de manera incompatible con tales fines.*."

pueden diferenciarse entre las que exigen alguna forma de autorización previa, sin poder procesar datos personales hasta haber obtenido el permiso, y las que prescinden de dichos controles.

El sistema de licencia, consistente en solicitar permiso previo para crear un sistema de información que recoja, almacene, procese y manipule datos personales permite asegurar un riguroso control del cumplimiento de la ley[49]. Pronto quedó patente que suponía un incremento innecesario de burocracia y también de costes[50], lo que ha hecho que muchos paises no lo apliquen, adoptando como alternativa para asegurar la necesaria información el sistema de declaración. De acuerdo con dicho sistema, todo fichero que contenga datos personales debe ser descrito en una declaración, que se comunica a las autoridades quedando el sistema autorizado salvo comunicación en sentido contrario. La declaración queda a disposición de la autoridad responsable, quien puede seguir el desarrollo del fichero, sometiendo a una inspección más detallada aquellos que considere encierran un mayor riesgo de violar la intimidad de los individuos.

En Francia y Dinamarca el sector público está sujeto a licencia. Siguiendo procedimiento declarativo en relación con el procesamiento automático de datos personales del sector privado. La Ley danesa, a diferencia de la francesa, somete a declaración, no los sistemas o ficheros, sino determinadas actividades como estudios crediticios, servicios de buzoneo directo y empresas de servicios informáticos. En Luxemburgo todos los bancos de datos que contengan datos personales deben ser autorizados por el Ministro de Justicia con el consejo del Comité Consultivo. Dicho Comité ha manifestado la necesidad de revisión, de tal política ya que considera que dicha autorización debería ser abandonada para el sector privado y ser sustituida por un procedimiento de declaración.

La ley española, establece para la creación de ficheros de titularidad privada la obligación de notificar previamente a la Agencia de protección de Datos y en relación a los ficheros de titularidad pública indica que deberán realizarse por medio de disposiciones generales publicadas en el BOE, o diario oficial correspondiente.

Todas las leyes tutelares que se analizan contemplan un sistema de registro, donde se recoge información sobre los ficheros que contenienen datos

■ 49 La opción de crear este registro de registros supone una aportación a la transparencia del proceso de datos, para verificar que los datos se destinarán al fin previsto. Ver BURKERT, Herbert.: *Transborder Data Flow, Data Protection and the EEC: Towards an EEC Directive on Data Protection*, RCIE, 1990, p. 8.

■ 50 RODOTA, S.:*Policies and perspectives on Data Protection*, en COUNCIL OF EUROPE. *Beyond 1984. op. cit. p.18*

personales para la consulta de ciudadanos y autoridades. En líneas generales cabe afirmar que, el sistema de la autorización previa se va sustituyendo por la fórmula de declaración, que, a su vez, es sustituido por la fórmula de simple inscripción en el registro, sin intervención de decisión alguna por parte de las autoridades en protección de datos. El sistema de registro es también objeto de revisión, dirigida a reducir los supuestos en que es preciso registrar[51]. Las razones que aparentemente explican esta evolución son dos: el modelo inicial se diseñó con el objeto de regular una realidad totalmente nueva, hasta cierto punto desconocida y, también, porque era factible con la realidad tecnológica del momento[52].

Conclusiones.

La implantación discontinua, pero generalizada, de las Nuevas Tecnologías de la Información ha supuesto una amenaza para los Derechos Fundamentales del hombre y ha desembocado en la articulación de leyes tutelares de los sujetos de datos, con la intención de lograr un control mínimo pero eficaz que no bloqueara el desarrollo tecnológico y económico. Desde una perspectiva estrictamente europea, todas las leyes de protección de datos tienen en común las siguientes condiciones: el reconocimiento del carácter excepcional (*Unique Nature*) del procesamiento de datos personales; la inequívoca manifestación de los propósitos de los requerimientos para procesar informaciones personales; la continua revisión actualizadora de las normas y la previsión de una autoridad independiente de control[53].

La evolución normativa en materia de protección de datos se ve doblemente influenciada por la creciente integración comunitaria y la imparable internacionalización de los servicios informáticos y telemáticos. En la Comunidad Europea convergen casos de precoz articulación normativa en paises como Alemania, Francia, Dinamarca y Luxemburgo, con paises donde la temprana preocupación se dilata en el tiempo hasta conseguir un entramado legislativo en protección de datos particularmente, el Reino Unido y Paises Bajos. Por su parte, Portugal y España aprovecharon que sus constituciones fueron redactadas en una época sensible en cuestiones referentes a la protección de

- 51" *I attach considerable wight (...) to the strong feeling, commonly expresed (by U.K. bussiness interests) that small routine commercial entreprises are not undertaking activities of major data protection significance. They ought to comply with the Data Protection Principles, but if at all possible, be be relieved of the bureaucratic burden of registration*", The Registrar's Fith Report. June 1989. p.78-79.
- 52 Ver SIMITIS, S.: *New Trends in National and International Data Protection Law.* en DUMORTIER, J. (Ed.): *Recent developments in data privacy law. ICRI Conference.* Leuven University Press, Lovaina, 1992, p. 19
- 53 SIMITIS, S.: *Reviewing Privacy in an Information Society,* Univ. Pensilv. Law Rev., vol. 135, nº 3, pp. 107 y ss.

datos y reflejaron su preocupación existente , pero dada su inquietud inicial resulta sorprendente su lentitud a la hora de legislar. Por último, paises que han conocido varios proyectos legislativos sin cuajar hasta el momento como Italia y Grecia.

Las primeras leyes eran rígidos instrumentos que surgieron como reacción ante las nuevas situaciones originadas por la la utilización de la informática, caracterizada por una tecnología hoy casi obsoleta: unos bancos de datos muy caros, escasos, voluminosos y, por lo tanto, fácilmente localizables. La práctica consistió en una ley general y un órgano vigilante.

El Convenio del Consejo de Europa de 1981 marcó una nueva etapa, que inició la promulgación de nuevas leyes y la revisión de las normas de la primera generación, esta segunda generación de leyes de protección de datos parten de la experiencia adquirida en la década anterior y se enfrentan con otra sensibilidad al empuje de las nuevas tecnologías de la información. Estas normas tutelares se caracterizan por la búsqueda de una simplificación con respecto a las de la anterior fase, abandonando gradualmente mecanismos previos como, por ejemplo, la licencia. Se opta por una sectorización más detallada, por una tendencia a la autorregulación y por el uso progresivo de sanciones civiles para reforzar la protección de datos. Se percibe una búsqueda de equilibrio entre la necesaria utilización de sistemas de información de todo tipo y la protección de la intimidad, manteniéndose la estructura de una autoridad para la protección de datos que resuelva los conflictos existentes.

Todos los estados miembros de la Comunidad Europea que actualmente disfrutan de leyes tutelares han firmado el Convenio del Consejo de Europa, primer tratado multilateral jurídicamente obligatorio sobre la materia, que subordina la libre circulación de datos personales a la presencia de un nivel mínimo de protección equivalente entre las partes. Sin embargo, la firma del Convenio por parte de los Estados Miembros no ha proporcionado la protección homogénea necesaria, debido principalmente a que el Convenio establece unos principios mínimos de protección permitiendo a las partes contratantes ofrecer un nivel de protección más elevado; a que los estados pueden excluir categorías enteras de ficheros a la aplicación de las normas tutelares y las medidas para que tales principios sean operativos en la práctica son adoptadas en base al ordenamiento interno de cada estado. Además, el Convenio no establece reglas sobre conflicto de leyes, ni un Tribunal supranacional u otro organismo similar al que puedan referirse las partes contratantes. Consecuentemente, la superación de estos problemas urge la pronta aprobación de la Directiva Comunitaria, que establezca una armonización de alto nivel de protección en todos los estados comunitarios

Bibliografía.

La principal bibliografía para el análisis de las legislaciones de protección de datos han sido de dos tipos: fuentes y doctrina.

Entre las fuentes destacan: Varias versiones en inglés de las leyes de protección de datos de Paises Bajos, Portugal, Irlanda, el Reino Unido en los libros de las leyes o como suplementos del TDR (Transnational Data Report). Además de la recopilación en castellano de legislación en el tema:

Presidencia del Gobierno/Secretaría General Técnica /Servicio Central de Informática. *IBI. Oficina Intergubernamental para la Informática.* Servicio Central de Publicaciones. Doc. Informática. Madrid. 1977.

Presidencia del Gobierno/Secretaría General Técnica /Servicio Central de Informática. Informática. *Leyes de Protección de datos.* Servicio Central de Publicaciones. Madrid. 1977.

Presidencia del Gobierno/Secretaría General Técnica /Servicio Central de Informática. *Flujo Internacional de datos.* Servicio Central de Publicaciones. Madrid. 1982.

Presidencia del Gobierno/Secretaría General Técnica /Servicio Central de Informática. Informática. *Leyes de Protección de datos (II). Austria, Dinamarca 1 y 2, Francia, Noruega.* Servicio Central de Publicaciones. Madrid. 1983.

Conferencia Internacional. *Problemas de la legislación en materia de protección de datos. Actas y documentos.* Servicio Central de Publicaciones. Madrid. 1984.

Explanatory Report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series, No.108. Council of Europe. Strasbourg, 1981.

Como diccionario de consulta en el tema: TRANSLATION DIVISION OF THE CEC. *Data Protection - Data Security - Privacy.* Terminología trilingüe: Alemán / Inglés / Francés. Office des publications officielles des Comm. Europ. Luxembourg. 1981.

Entre los principales textos de la doctrina:

BING, J.: *Impact of Developing Information Technology on Data Protection Legislation.* OECD-ICCP (86) 5, París 1986.

BING, J.; *Reflections on Data Protection Policy for 1992,* En *Access to the Public Sector Information, Data Protection and Computer Crime.* Comission of the European Communities / Council of Europe. Luxemburgo 27-28 marzo de 1990.

BOIX REIG, J.: *Protección Jurídico penal de la intimidad e informática.* Congreso sobre Derecho Informático, 22-24 de Junio, Zaragoza, 1989.

BOURN, C.; BENYON, J.: *Data Protection.* Perspectives on Information Privacy Contributions made to a Conference at the University of Leicester. University of Leicester. Leicester. 1983.

CAMERON, E.; BLUME, P.: *Data Protection Law in the United Kingdom and Denmark.* University of Leicester, Leicester, 1988.

CARRASCOSA LOPEZ, Valentín: *Derecho a la intimidad e informática.* En Informática y Derecho, nº 1, 1992.

CLARK, R.; LINEHAM; D. C.; . *Data Protection Law in Ireland.* The Round Hall Press. Dublin. 1989.

CHALTON, S. N. L. y GASKILL, S. J.: *Enciclopedia of Data Protection.* Sweet & Maxwelll, Londres, 1989.

DENNINGER, E.: *El derecho a la autodeterminación informativa,* en PEREZ LUÑO, A. E, *Problemas actuales de la documentación y la información jurídica.* Ed. Tecnos. Madrid, 1987.

ELLGER, R.: *European Data Protection Law and the Free Transborder Flow of Information,* en MESTMÄCKER, Ernst-Joachim (Ed.): *"The Law and the* Economics of Transborder Telecommunications". Nomos Verlagsgeseellschaft. Baden-Baden. 1987.

GARCIA LLOVET, E.: *,Empresa informática y libertad de información,* TELOS. 133-139.

GARZON CLARIANA, G.: *La protección de los datos personales y la función normativa del consejo de Europa,* Revista de Instituciones Europeas, Enero-Abril. 1981.

GARZON CLARIANA, G.: *Informatización de la sociedad y derecho de gentes,* Cursos de derecho internacional de Vitoria-Gasteiz, 1983.

GEBHARDT, H. P.: *La protección de datos en paises industrializados. Principios y situación jurídica,* TELOS (18), julio-agosto 1989.

HARREMOES, Erik: *Summary of Conclusions.* XIIIth Conference of Data Protection Commissioners, Strasbourg, 2-4 October 1991. p. 2

HEREDERO HIGUERAS, M.: *Anteproyecto Español de Ley Orgánica de regulación del uso de la informática, cinco años después,* CONGRESO SOBRE DERECHO INFORMATICO, 22-24 de Junio, Zaragoza, 1989.

HEREDERO, M.: *La informática y el uso de la información personal.* en RIVERO, A. M. y SANTODOMINGO, A.: *Introducción a la informática jurídica.* Fundesco, Madrid, 1986.

JOINET, L.: *Orientaciones principales de la Ley francesa relativa a la informática, los ficheros y las libertades.* Servicio Central de Publicaciones / Presidencia del gobierno. Presidencia del Gobierno, Secretaria General Técnica. Separata del núm. 178. Madrid, abril-junio 1978.

LOSANO, M. G.: *Los orígenes del "Data Protection Act" inglesa de 1984,* en LOSANO, M. G.; PEREZ LUÑO, A. E.; GUERRERO MATEUS, Mª F.: «*Libertad informática* .... pp. 9-60.

LOSANO, M. G.; PEREZ LUÑO, A. E.; GUERRERO MATEUS, Mª F.: «*Libertad informática y leyes de protección de datos personales*». Centro de Estudios Constitucionales. Madrid. 1989.

LOSANO, Mario G, *Un proyecto de ley sobre protección de datos personales en Italia.* En LOSANO, M. G.; PEREZ LUÑO, A. E.; GUERRERO MATEUS, Mª F.: «*Libertad informática*.... pp. 61-94.

MADRID CONESA, F.: *Derecho a la intimidad, Informática y estado de derecho.* Universidad de Valencia. Valencia, 1984.

MARCELO, J.: *Libertades e informática en Europa. Parte I: Antecedentes.* NOVATICA nº 94

MARCELO, Julián: *Libertades e informática en Europa. Parte II: Década actual y bases jurídicas.* NOVATICA nº 95

MORALES PRATS, F.: *La tutela penal de la intimidad: privacy e informática.* Ediciones Destino Barcelona 1984.

MURILLO DE LA CUEVA, P. L.: *El derecho a la autodeterminación informativa, Tecnos.* Madrid, 1990.

NUTGER, A.: *Transborder Flow of Personal Data within the EEC,* Kluwer, Amsterdam, 1990,

PEERS, E.; BUCKLEY, B.: *Computers and Data Protection.* Deloitte, Haskins & Sells. London. 1988.

PEREZ LUÑO, A. E.: *Nuevas tecnologías, sociedad y derecho.* Fundesco, Madrid, 1987,

PEREZ LUÑO, A. E., *Los derechos humanos en la sociedad tecnológica,*en LOSANO, M. G.; PEREZ LUÑO, A. E.; GUERRERO MATEUS, Mª F.: «*Libertad informática....* pp. 133-185.

PIÑOL i RULL J. L.: *Los servicios proporcionados por las nuevas tecnologías de la información.* Anuario CIDOB, 1990. pp. 209-235.

RODOTA, S.: *Policies and perspectives on Data Protection,* En COUNCIL OF EUROPE, *Beyond 1984,* Council of Europe, Strasbourg ,1985, pp. 13-42.

ROMEO CASABONA, C.M.: *Poder informático y seguridad jurídica.* Editorial Fundesco. Madrid, 1986, p. 28.

SEIPEL, P. (ed.) et al.: *From Data Protection to Knowledge Machines.* Kluwer Law and Taxation Publishers. Deventer. 1990.

SELMER, K: *Data Protection Policy.* en SEIPEL, P.: *From Data Protection to Knowledge Machines.* Kluwer, Computer Law Series/5. Deventer 1990, pp. 11-28.

SIMITIS, Spiros: *General Report,* En COUNCIL OF EUROPE, *Beyond 1984,* Council of Europe, Strasbourg ,1985, pp. 105-117.

SIMITIS, S.: *New Trends in National and International Data Proteciton Law.* en DUMORTIER, J. (Ed.): *Recent developments in data privacy law. ICRI Conference.* Leuven University Press, Lovaina, 1992,

VANDENBERGHE, G. P. V. (Ed.): *Advanced Topics of Law and Information Technology.* Kluwer Law and Taxation Publishers. Deventer, 1989.

Ley Orgánica de Protección de Tratamiento Datos de Carácter Personal (LORTAD)

INTRODUCCION: HYPERIUS

AUDILIO GONZALES AGUILAR

Doctor en Derecho e informática jurídica y miembro del grupo de investigación de la Universidad de Montpellier.

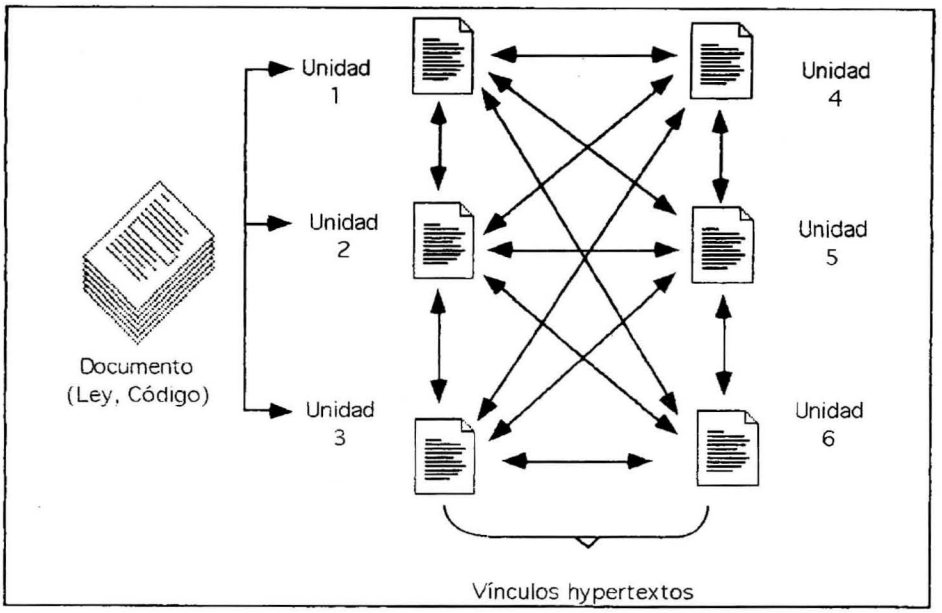
El sistema hypertexto se sirve de las posibilidades técnicas del ordenador para la búsqueda de los pasajes o conceptos importantes de un documento. Con el método hypertexto no se busca imitar un libro electrónico sino aprovechar las ventajas de la informática para superar las dificultades inherentes al documento escrito (acceso secuencial, volúmen del libro).

La principal característica del hypertexto es la de favorizar la explotación no secuencial de los documentos. En qué consiste esta lectura/escritura no secuencial. El usuario tiene la posibilidad de seguir diferentes referencias que conducen su razonamiento de manera asociativa. Estas referencias son determinadas a través de todo el documento tratado y constituyen verdaderas entradas a diferentes niveles de información.

En el caso del escrito, la estructura del documento es lineal y estática, y no corresponde a nuestros procesos mentales asociativos. El sistema hypertexto representa una alternativa electrónica que busca romper la linearidad de los libros tradicionales.

Los libros y casi todos los sistemas informáticos tratan el texto y la información de manera lineal, es decir, letra por letra o palabra por palabra, esta

operación no corresponde a la forma como las personas tratan los documentos o la información. El individuo efectúa asociaciones mentales entre unidades de información aparentemente sin ningún vínculo entre ellas. El cerebro humano es así capaz de pasar rápidamente de una idea a otra, de comparar, de aproximar y disociar temas, conceptos, hechos. Actualmente los nuevos sistemas de tratamiento de la información documentaria buscan reproducir de manera cercana el modo de pensar humano y el sistema neuronal.



Los sistemas hypertextos permiten el vínculo o lazo entre las diferentes unidades de información, permitiendo al usuario decidir que tipo de relación o vínculo debe crear y cuando debe hacerlo.

La palabra hipertexto creada por T. H. Nelson define "la lectura no secuencial". Intentemos explicar el carácter no secuencial o no lineal de la lectura para comprender exactamente la dimensión del concepto hipertexto. Sabemos por los trabajos de linguística de Ferdinand de Saussure que la lengua tiene un carácter lineal en el sentido en que el sonido se desarrolla en el tiempo y el signo escrito en el espacio. Una lectura tiene sentido y se hace coherente por el hecho de leer las palabras una seguida de las otras. Así no es imposible pensar en una lectura "no secuencial". ¿Cómo interpretar los términos de T. H. Nelson?

El usuario de un sistema hypertexto podrá proceder en todo momento hacer el análisis y a valorar de manera técnica los documentos, para finalmente guardar o excluir los documentos pertinentes que le dan satisfacción en su investigación o trabajo documentario. El Hypertexto propone una aproximación, una escritura y una exploración dinámica del documento.

El programa Jurilien® es un sistema que permite desarrollar bases de datos utilizando los principios Hypertextos.

Convenciones gráficas del presente manual.

Con el fin de utilizar al máximo este manual a continuación usted encontrará las indicaciones de cada una de sus partes y su característica.

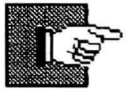
1. presentación del programa en pantalla

Un texto o una gráfica con ésta presentación (enmarcado en doble línea, muestra como aparecerá el programa Jurilien® en la pantalla del computador.

2. Presentación de las instrucciones y procedimientos a seguir para instalar o hacer funcionar los comandos del programa Jurilien® :

Este gráfico indica una instrucción o procedimiento a seguir en la utilización del programa. Sus instrucciones de debe seguir paso a paso para que su funcionamiento sea correcto.

3. Presentación de notas importantes:



Los parágrafos precedidos de ésta gráfica indican una nota a tener en cuenta. Son comentarios que pueden ser útiles para hacer más convivial o evitar errores de utilización del programa.

4. Presentación de las enumeraciones:

- El punto indica una enumeración.

5. Presentación de puntos de Atención:

Los párrafos precedidos de este signo llaman la atención sobre un aspecto particularmente importante.

Al final del manual se encuentra un resumen con todos los comandos y las posibilidad de utilizar el teclado del ordenador o el ratón.

INSTALACION

Material requerido:

Para la instalación del programa Hyperius® es necesario contar con:

- Un computador IBM PC, XT, AT, PS2 o compatible que tenga como mínimo un lector de disquettes (Drive) y un disco duro. El espacio utilizado por el programa dependará de la aplicación y la talla de los documentos.

- 512 K de memoria RAM

- Pantalla color VGA. (indispensable para visualizar los elementos hypertextos).

Instrucciones para su instalación

Introduzca el disquette en el lector de disquettes y escriba:

```
A: INSTALAC C:\Hyperius  y  RETURN (↵)
```

o igualmente

```
B: INSTALAC C:\Hyperius  y  RETURN (↵)
```

El programa automáticamente creará los directorios y sub-directorios necesarios para el buen funcionamiento del programa.

El programa Hyperius® puede ser ejecutado desde cualquier directorio del disco duro. Para esto es necesario crear un fichero *.BAT donde se puede incluir el comando MS-DOS PATH.

Funciones básicas

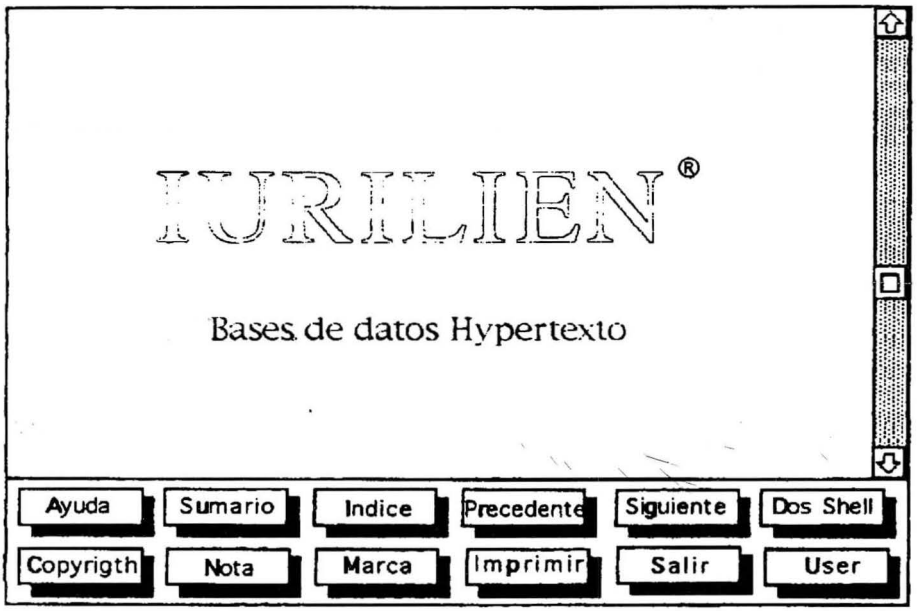
Este capítulo permitirá al usuario utilizar y consultar de una base hypertexto creada por Hyperius® .

Entrada

- Escribir en el DOS Hyperius® y luego validar con **Return** o Retorno

```
A:\> Hyperius
```

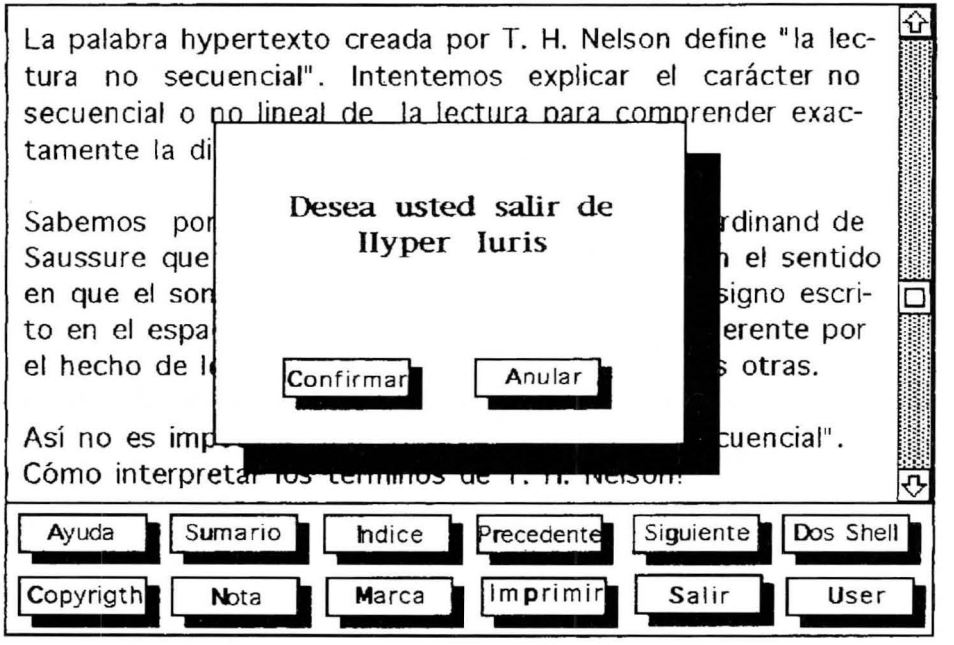
y luego validar con return o retorno ⏎



Salida

- Posicionar el cursor y pinchar con ayuda del ratón sobre el botón **Salir** o pulsar simultáneamente **ALT + S**

- En la pantalla aparecerá:



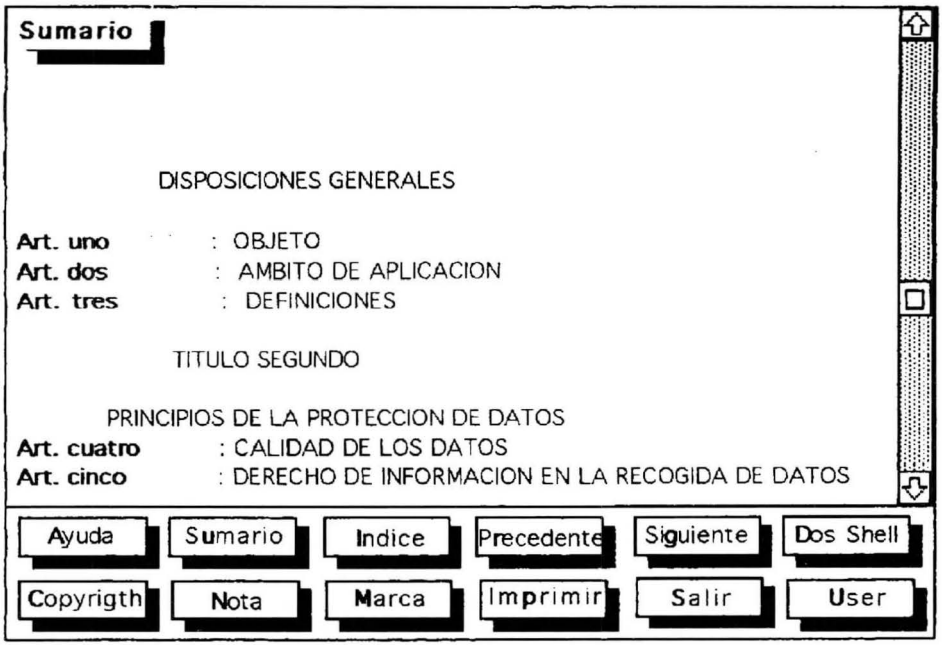
- Posicionar el cursor y pinchar con ayuda del ratón sobre el botón **Confirmar** o pulsar simultáneamente **ALT + C**

- Posicionar el cursor y pinchar con ayuda del ratón sobre el botón **Anular** o pulsar simultáneamente **ALT + A**

COMANDOS

Luego de haber lanzado Hyperius® una pantalla de presentación aparece:

Es importante precisar que el aspecto fundamental del Hypertexto es la posibilidad de establecer vínculos dinámicos entre los textos a partir de conceptos o frases previamente determinados. El texto toma así un carácter dinámico, al establecer las relaciones asociativas entre el texto.



Para poder avanzar no es necesario precisar ciertos términos que corresponden a varias de las funciones específicas al sistema hypertexto. Dentro de estos conceptos encontramos:

Botones: Los botones corresponden a las partes dinámicas del texto que se traducen en partes activas de la pantalla que establecen los vínculos asociativos entre las diferentes partes del texto.

Los botones materializan los diferentes tipos de vínculos entre las cartas o unidades conceptuales. Existen varios tipos de vínculos:

- **Los vínculos explícitos** : aquellos que se establecen entre conceptos directamente sin análisis. Ejemplo: "Serán aplicables a la presente convención las ***normas internacionales sobre la proteción de datos...***" el texto establece un vínculo explícito con la Convención Europea de 1981 sobre la proteción de datos. En este caso el botón precisa o explica más en detalle una información contenida en el texto. El mismo caso se presenta con las concordancias entre lso artículos de una ley que reenvían explícitamente a otro texto o a otro artículo de la misma ley.

- **Los vínculos implícitos** : Pueden presentarse igualmente relaciones entre el texto del documento que implican un análisis y que ponen en evidencia las relaciones asociativas en el documento. Es el caso por ejemplo cuando un artículo de una ley dispone que " ... En caso de ser contraria la decisión al demandante queda abierta la posibilidad de intentar ***todo recurso***". La expresión "todo recurso" *me hace pensar* en los tipos de recursos, su trámite, oportunidad, etc.

  Este tipo de vínculos implícitos supone un análisis previo por parte del creador de la bases de datos hypertexto. En el caso de bases de datos de leyes o códigos este tipo de relación se hace evidente en el caso de la referencia a la jurisprudencia y a la doctrina de cada artículo o de un punto determinado del derecho.

Ventanas: Son las diferentes partes en que se puede dividir la pantalla del ordenador y que pueden contener instrucciones de control o información preparada por el usuario del programa. Cada ventana corresponde a determinadas funciones hypertexto y contiene diferentes partes activas para la realización de los vínculos dinámicos.

La pantalla de Hyperius® está dividida en dos ventanas:

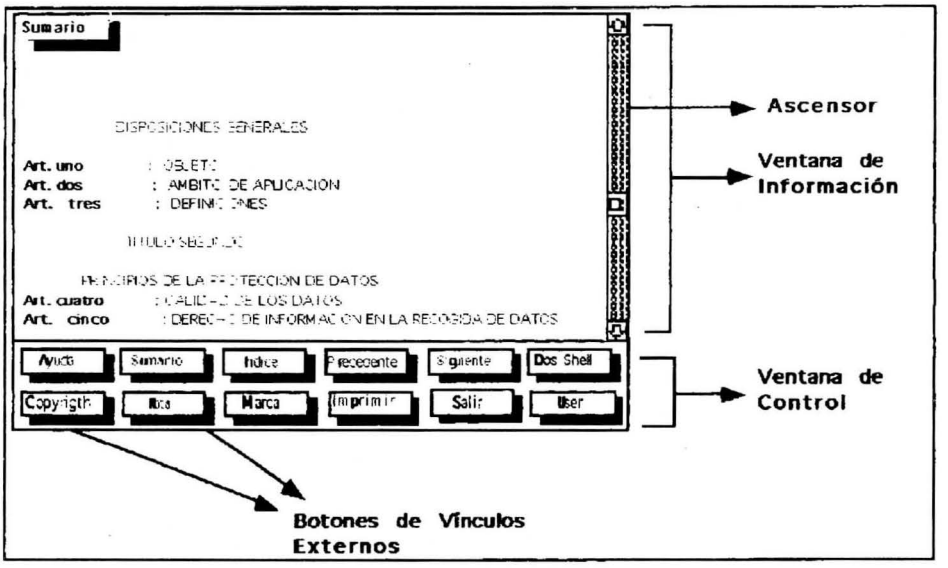
- ***La ventana de información*** : que contiene la unidad de información, la parte del texto seleccionado en una carta;

- ***La ventana de control*** : que contiene los botones que permitirán navegar por la información contenida en la base Hypertexto.

Cartas: Corresponden a las unidades conceptuales definidas por el conceptor de la base hypertexto que debe previamente analizar la información a entrar en el sistema. Cada carta corresponde a la visualización de la pantalla de la computadora con la ventaja que utilizando los ascensores de desfilamiento situados en el lado derecho de la pantalla es posible entrar en una carta o una unidad conceptual varias páginas de información.

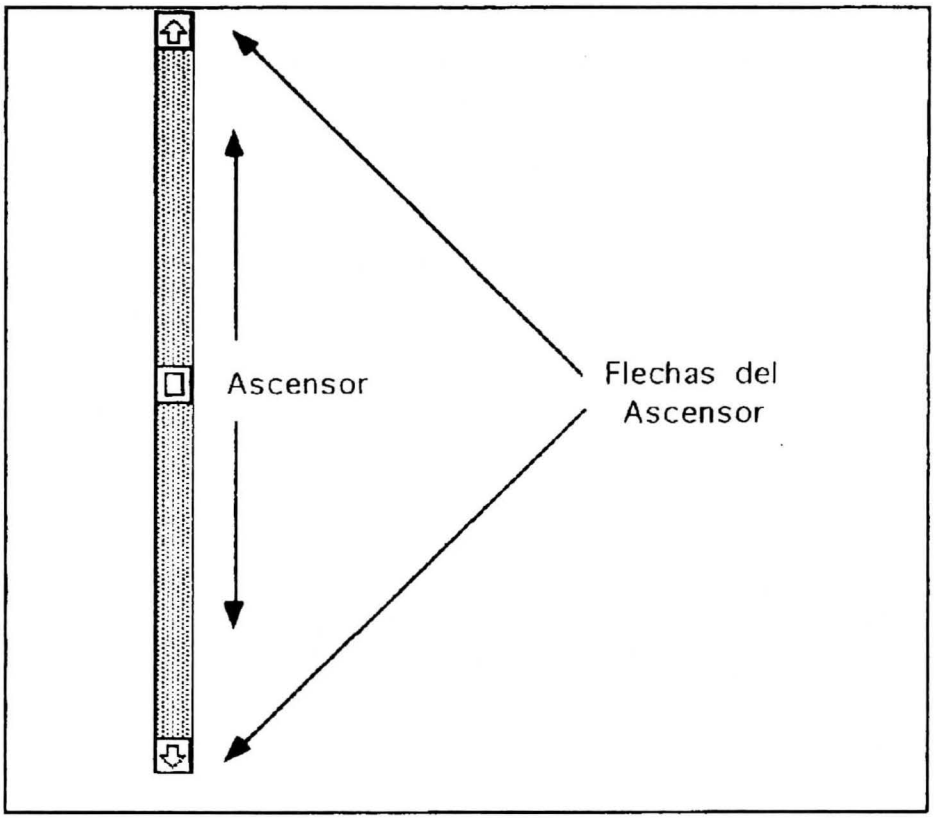
La unidad de información o carta puede ser superior a la superior a la talla de la pantalla, pues existe al lado derecho de la ventana un ascensor que permite desplazarse en la ventana.

Así es posible incluir un artículo de la ley que sea contenido en varias pantallas (o páginas)



Para hacer desfilar el texto en pantalla se debe proceder de la siguiente manera :

- *Utilizando el ratón* : Se posiciona el cursor en el ascensor en la flecha arriba o abajo que aparecen en la pantalla y se pincha cada vez que se desea descender o subir el texto que aparece en pantalla.



Bases: Se constituyen con las diferentes unidades de información o cartas del programa. Cada base es independiente y constituye en si misma un sistema con todas las relaciones establecidas entre las diferentes cartas.

En programa permite crear multiples bases hypertextos interrelacionadas entre si. Esto permite una facilidad para la estructuración de la información.

NAVEGACION

Esta es una de las principales características del sistema hypertexto y consiste en la posibilidad ofrecida al usuario de la base de datos hypertexto realizar una lectura secuencial y lineal o una lectura no secuencial o en saltos a través de la información.

El carácter no secuencial de la lectura está dado por la posibilidad de "navegar" por la información. Esta información está constituída por textos, frases, fichas, sin seguir un plan establecido o un camino determinado. El ejemplo para ilustrar este tipo de lectura es la obra de Julio Cortázar "La rayuela". En esta novela, Cortázar propone al lector alternativas de lectura de su obra: El lecto puede leer en orden todos los capítulos del libro, o bien puede leer la versión corta que termina en la mitad del libro, o finalmente puede leer el libro a través de un camino propuesto por el autor en el cual del capítulo 1 pasa por ejemplo al capítulo 5 y de este al 20 y así sucesivamente.

FUNCIONES ESPECIFICAS

El programa Hyperius® presenta en la ventana inferior una serie de funciones estándares de los sistemas hypertextos para permitir la navegación a través de la información. Estas funciones buscar realizar la consulta de un libro o enciclopedia electrónica. Así hemos mantenido ciertos mecanismos de consultas existentes en el soporte papel como son el índice o el sumario, mejorados en cuanto el usuario de la base tiene acceso desde todos las cartas de información a estas funciones. Además de estas funciones tradicionales el creador de la base de datos puede incluir todos los botones necesarios para la realización de los vínculos hypertexto.

A continuación presentaremos cada una de la funciones específicas y la manera de utilizarlas a través del teclado, los comandos, las teclas de función y el empleo del ratón.

Ayuda

Este botón permite al usuario acceder a una ayuda sobre la estructura del programa Hyperius®, así como de las funcionalidades y comandos del mismo. (Ver supra tabla anexa).

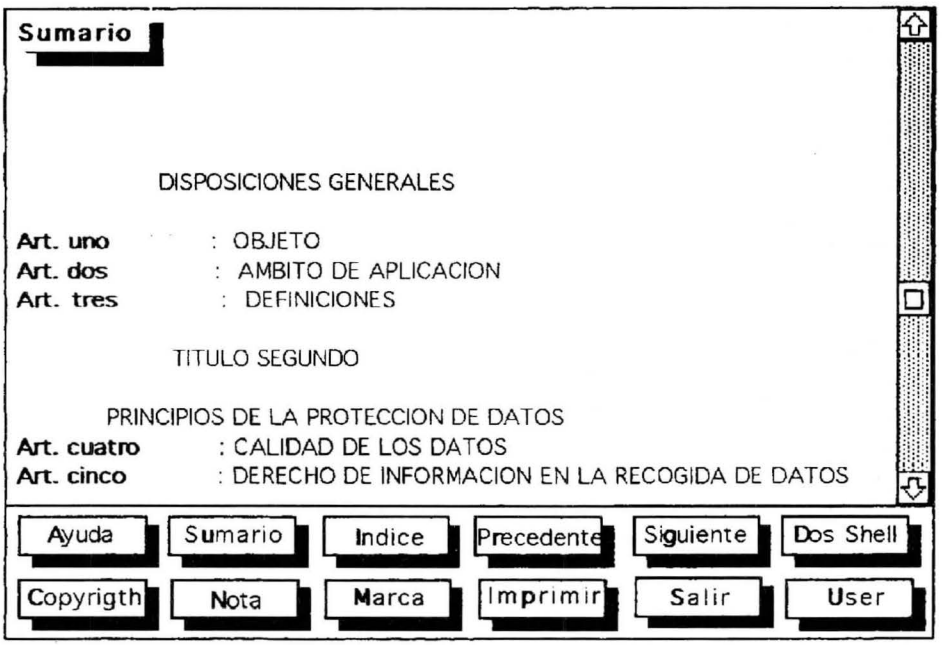
Modo de utilización: se puede acceder a la ayuda del programa de tres formas:

- *Utilizando el ratón*: se posiciona sobre el botón Ayuda que se encuentra en la parte inferior de la pantalla y se pincha una vez.
- *Utilizando el teclado*: se pulsa al mismo tiempo las teclas **ALT + A**
- Utilizando la *tecla función* ***F1***.

Sumario

Esta función permite al usuario una vez entra a la base de datos, determinar de manera general el contenido de la base. El sumario responde al acceso directo a cada una de las cartas de la base, estructuradas de acuerdo a materia tratada. Ejemplo: el sumario del código de procedimiento civil será la descripción de cada uno de los libros, capítulos y secciones, conteniendo igualmente cada uno de los artículos. El interés de este tipo de sumario consiste en el acceso directo a la información estructurada en una tabla de materias.

Este botón Sumario puede enviar a una carta que permita incluir otra serie de cartas vinculadas entre sí y que permitirán diferentes niveles de consulta del sumario.



Modo de utilización: se puede acceder al Sumario de tres formas:

- *Utilizando el ratón*: se posiciona sobre el botón Sumario que se encuentra en la parte inferior de la pantalla y se pincha una vez.

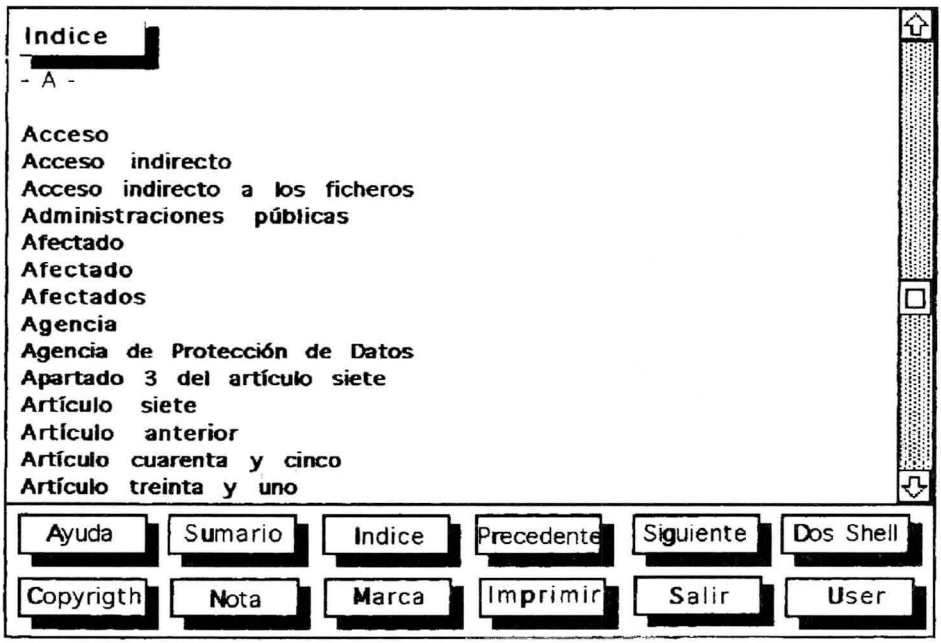
- *Utilizando el teclado*: se pulsa al mismo tiempo las teclas **ALT + U**
- Utilizando la *tecla función F2*.

El sumario es consultable a todo momento en la consulta de la base.

Indice

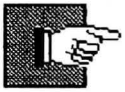
Presenta una lista de palabras o de conceptos jurídicos tomados de la base hypertexto por la cual el usuario puede acceder directamente a la carta o unidad de información deseada. Se puede consultar en todo momento y desde cualquier punto de consulta de la base de datos.

Este botón Indice puede enviar a una carta que permita incluir otra serie de cartas vinculadas entre sí y que permitirán diferentes niveles de consulta del mismo. Igualmente puede contener diversos tipos de indice (temático, de materias, alfabético, etc.)



Modo de utilización: se puede acceder al Indice de tres formas:

- *Utilizando el ratón* : se posiciona sobre el botón Indice que se encuentra en la parte inferior de la pantalla y se pincha una vez.
- *Utilizando el teclado* : se pulsa al mismo tiempo las teclas **ALT + I**
- Utilizando la *tecla función* ***F3***.



- Para utilizar el índice se puede utilizar el teclado.
- Una vez el programa abre el Indice, se puede buscar por orden alfabético todos las palabras o voces que se han utilizado como botones de vínculo hypertexto en la base de datos.
- El índice alfabético es creado automáticamente por el programa de creación de bases de datos hypertexto Iuriedit®.
- El usuario tiene la posibilidad de acceder directamente alfabéticamente pulsando la tecla que corresponda a la primera letra del tema palabra o voz que desee consultar.

Precedente

Este botón permite regresar de manera contínua a través de todas las cartas que se han presentadò en pantalla y que han sido recorridas en la consulta por el usuario.

Modo de utilización: se puede acceder de tres formas:

- *Utilizando el ratón* : se posiciona sobre el botón "Precedente" que se encuentra en la parte inferior de la pantalla y se pincha una vez.
- *Utilizando el teclado* : se pulsa al mismo tiempo las teclas **ALT + r**
- Utilizando la *tecla función* ***F4***.

Siguiente

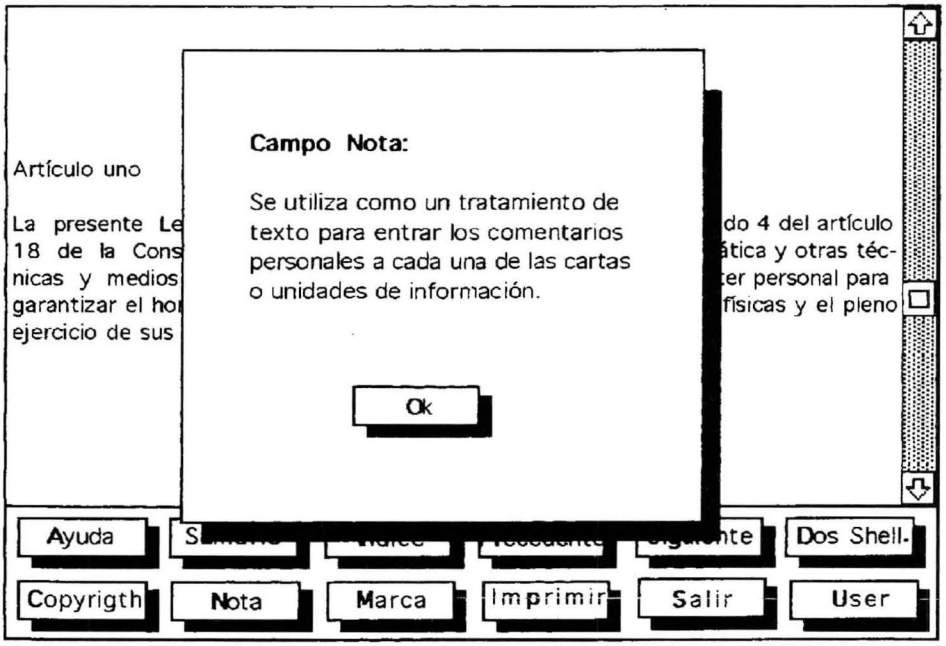
Esta función permite al usuario "navegar" a través de todas la cartas que ha consultado. Esta función es complementaria a la función desarrollada por el botón "Precedente".

Modo de utilización: se puede acceder de tres formas:

- *Utilizando el ratón* : se posiciona sobre el botón "Siguiente" que se encuentra en la parte inferior de la pantalla y se pincha una vez.
- *Utilizando el teclado* : se pulsa al mismo tiempo las teclas **ALT + g**
- Utilizando la *tecla función F5.*

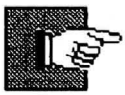
Nota

Este botón permite acceder a un editor que sirve a la creación de comentarios personales sobre cada carta o unidad de información.



Modo de utilización: se puede acceder de tres formas:

- *Utilizando el ratón* : se posiciona sobre el botón "Nota" que se encuentra en la parte inferior de la pantalla y se pincha una vez.
- *Utilizando el teclado* : se pulsa al mismo tiempo las teclas **ALT + N**
- Utilizando la *tecla función F7.*



Para entrar la nota se utiliza como un procesador de texto.

- Es necesario hacer retorno a cada una de la líneas.
- Para terminar es necesario pinchar sobre el botón **OK** que se encuentra en la parte inferior de la ventana . Es posible salir o anular la utilización de la nota utilizando la tecla **Esc** .

- Este campo es limitado a la ventana que se presenta en pantalla. Su función está limitada a ser utilizado como un pequeño memorando de notas del texto principal y constituye una ayuda importante al usuario en cuanto le permite elaborar comentarios o notas en cada una de las unidades de información.

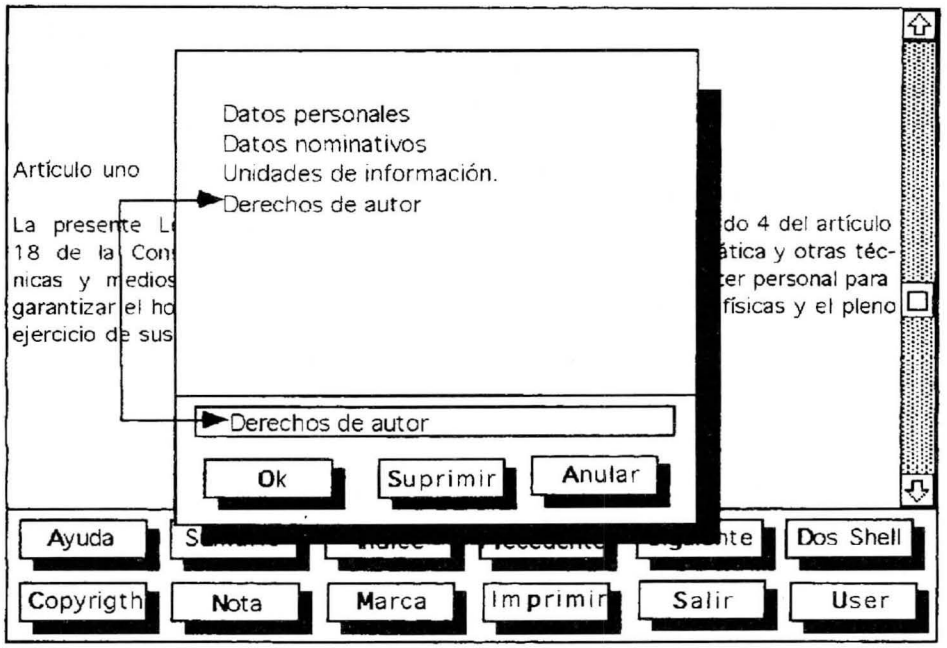
Marca

Este botón permite acceder a una lista en la cual el usuario puede atribuir un nombre a la carta o cartas que consulta. Funciona como un separador de páginas de un libro.

En la ventana que se presenta en pantalla se incluyen tres botones:

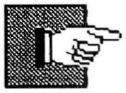
- ***Botón OK,*** que permite grabar una Marca entrada por el usuario y al mismo tiempo cerrar la ventana de marca.
- ***Botón Suprimir,*** que permite suprimir la Marca contenida en la lista previamente seleccionada con el cursor utilizando las flechas arriba-abajo del techado o pinchando directamente con el ratón sobre la marca seleccionada.

- *Botón Anular,* que cierra automáticamente la ventana de Marca.



Modo de utilización: se puede acceder de tres formas:

- *Utilizando el ratón* : se posiciona sobre el botón "Marca" que se encuentra en la parte inferior de la pantalla y se pincha una vez.
- *Utilizando el teclado* : se pulsa al mismo tiempo las teclas **ALT + M**
- Utilizando la *tecla función F8.*



- Para entrar la marca se utiliza el teclado.
- Es necesario entrar un nombre que no sea utilizado en la base hypertexto.
- Para terminar es necesario pinchar sobre el botón **OK** que se encuentra en la parte inferior de la ventana.
- La marca entrada aparecerá en la parte superior de la ventana en la lista.

- Es posible suprimir una marca, seleccionándola con ayuda del ratón o con ayuda de la las **flechas arriba y abajo** de desplazamiento del cursor. Una vez seleccionada se pincha sobre el botón **Suprimir** o se utiliza el teclado pulsando al mismo tiempo las teclas **ALT + S**.

- Para cerrar la ventana de Marca, se puede utilizar el ratón, posicionándolo sobre el botón **Anular** o utilizando el teclado pulsando al mismo tiempo las teclas **ALT + A** . Es posible utilizar la tecla **Esc** para salir o anular la utilización de la ventana de Marca.

Imprimir

Este botón permite la impresión de la carta que se presenta en la pantalla. Su impresión se realiza directamente.

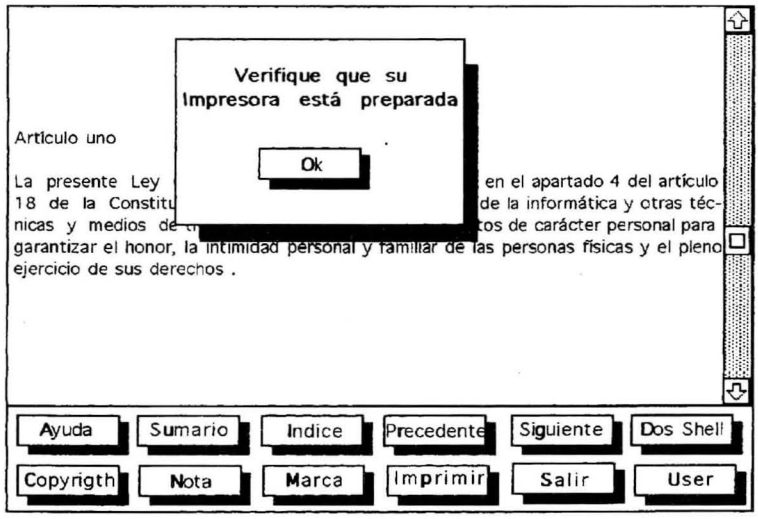
Modo de utilización: se puede acceder a esta función de tres formas:

- *Utilizando el ratón* : se posiciona sobre el botón "Imprimir" que se encuentra en la parte inferior de la pantalla y se pincha una vez.

- *Utilizando el teclado* : se pulsa al mismo tiempo las teclas **ALT + p.**

- Utilizando la *tecla función* ***F9***.

En la pantalla aparecerá:



Dentro de esta pantalla aparece un botón **OK** el cual con ayuda del ratón da comienzo a la impresión. Se pueden utilizar igualmente a nivel de teclado la tecla **RETURN** o la tecla **Esc** para lanzar la impresión.

La impresión se realiza sobre toda la información contenida en la carta o en la unidad de información así esta no se presente en su totalidad en la pantalla, es decir que la información contenida sea mayor a la pantalla.

FUNCIONES Y COMANDOS DE IURILIEN

Botón	Tecla función	Comando	Comentario
Ayuda	F1	ALT + A	Presenta la ayuda del programa
Sumario	F2	ALT + S	Presenta la tabla de materias o la estructura de la base de datos
Indice	F3	ALT + I	Visualiza el índice en pantalla.
Precedente	F4	ALT + r	Regresa a la carta anterior
Siguiente	F5	ALT + g	Avanza a la carta siguiente
Dos Shell	- -	ALT + D	Permite regresar al DOS
Copyrigth	F6	ALT + C	Derecho de autor
Nota	F7	ALT + N	Creación de notas personales
Marca	F8	ALT + M	Permite señalar un texto de la base
Imprimir	F9	ALT + p	Permite imprimir una carta
Salir	F10	ALT + S	Salir de IurilienO
User	- - -	ALT + O	Vínculo con otros programas

ANEXOS

ANEXO I

CONVENIO para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal. Hecho en Estrasburgo el 28 de enero de 1981.

"B.O.E." núm. 274, de l5 de noviembre de 1985

Preámbulo

Los Estados miembros del Consejo de Europa, signatarios del presente Convenio.

Considerando que el fin del Consejo de Europa es realizar una unión más estrecha entre sus miembros, en especial dentro del respeto de la supremacía del derecho, así como de los derechos del hombre y de las libertades fundamentales;

Considerando que es deseable ampliar el ámbito de las garantías de los derechos y libertades fundamentales de toda persona, en especial el Derecho a la intimidad, teniendo en cuenta la intensificación de la circulación internacional de los datos de carácter personal objeto de tratamientos automatizados;

Reafirmando al mismo tiempo su compromiso en favor de la Libertad de información, prescindiendo de las fronteras;

Reconociendo la necesidad de conciliar los valores fundamentales del respeto a la intimidad y a la libre circulación de la información entre los pueblos,

Han convenido en cuanto sigue.

CAPITULO PRIMERO

Artículo 1. *Objeto y fin.*

Fin del presente Convenio es garantizar, en el territorio de cada Parte, a toda persona física, cualesquiera que fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales y en especial de su Derecho a la intimidad, con relación al tratamiento automático de los datos de carácter personal que le conciernen ("protección de datos").

Artículo 2. *Definiciones.*

A los efectos del presente Convenio las expresiones que se relacionan tendrán los significados o contenidos que repectivamente se detallan:

a) "Datos de carácter personal" significará toda información concerniente a una persona física identificada o identificable ("interesado").

b) "Fichero automatizado" significará todo conjunto de informaciones que fuere objeto de un tratamiento automatizado.

c) "Tratamiento automatizado" comprenderá las operaciones siguientes, efectuadas en todo o en parte con ayuda de medios automatizados: almacenamiento de datos, aplicación a tales datos de operaciones lógicas o aritméticas, o de ambas, su modificación, borrado, recuperación o difusión.

d) "Responsable del fichero" significará la persona física o jurídica, autoridad pública, servicio u otro organismo que según la ley nacional fuere competente para decidir sobre qué clases de datos de carácter personal deben ser almacenados y qué operaciones deberán serles aplicadas.

Artículo 3. *Ambito de aplicación.*

1. Las partes se obligan a aplicar el presente Convenio a los ficheros y tratamientos automatizados de datos de carácter personal de los sectores público y privado.

2. Todo Estado podrá, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, o en cualquier otro momento ulterior, manifestar por medio de declaración dirigida al Secretario General del Consejo de Europa.

a) Que no aplicará el presente Convenio a determinadas clases de ficheros automatizados de datos de carácter personal, una lista de los cuales deberá ser depositada. En todo caso no incluirá en la lista los ficheros que según su Derecho interno estuvieren sujetos a disposiciones de protección de datos. En consecuencia, modificará dicha lista mediante una nueva declaración siempre que hubiere nuevos ficheros automatizados de datos de carácter personal que quedaren sujetos a su régimen de protección de datos.

b) Que aplicará asimismo el presente Convenio a informaciones relativas a grupos de personas, asociaciones, fundaciones, sociedades, corporaciones y cualquier otro organismo formado directa o indirectamente por personas fisicas, tuvieren o no personalidad jurídica.

c) Que aplicará asimismo el presente Convenio a los ficheros de datos de carácter personal que no fueren objeto de tratamiento automático.

3. El Estado que hubiere ampliado el ámbito de aplicación del presente Convenio por medio de una de las declaraciones aludidas en los apartados 2 b) o c) *supra*, podrá indicar en la expresada declaración que tales ampliaciones no se aplicarán más que a determinadas clases de archivos de carácter personal, cuya lista hubiere sido depositada.

4. La Parte que hubiere excluido determinadas clases de ficheros automatizados de carácter personal por medio de la declaración prevenida en el apartado 2 a), *supra*, no podrá exigir que el presente Convenio sea aplicado a tales clases de ficheros por una Parte que no los hubiere excluido.

5. Del mismo modo, la Parte que no hubiere procedido a una u otra de las ampliaciones previstas en los apartados 2 b) y c) del presente artículo no podrá prevalerse de la aplicación del presente Convenio a tal efecto con respecto a la Parte que hubiere procedido a tales ampliaciones.

6. Las declaraciones previstas en el apartado 2 del presente artículo surtirán efecto en el momento en que el Convenio entrare en vigor con respecto al Estado que las hubiere formulado, siempre que este Estado las hubiere hecho en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, o tres meses después de la recepción de las

mismas por el Secretario General del Consejo de Europa si hubieran sido formuladas en un momento posterior. Tales declaraciones podrán ser retiradas en todo o en parte por medio de notilcación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto tres meses después de la fecha de recepción de la notificación.

CAPITULO II

Principios fundamentales de la protección de datos

Artículo 4. *Obligaciones de las Partes.*

1. Cada Parte adoptará en su Derecho interno las medidas necesarias para dar cumplimiento a los principios fundamentales de protección de datos enunciados en el presente capítulo.

2. Tales medidas deberán ser adoptadas lo más tarde en el momento en que el presente Convenio entrare en vigor con respecto a la Parte.

Artículo 5. *Calidad de los datos.*

Los datos de carácter personal que fueren objeto de un tratamiento automatizado deberán ser:

a) Obtenidos y elaborados leal y lícitamente.

b) Registrados para unos fines determinados y legítimos y no utilizados de manera incompatible con tales fines.

c) Adecuados, pertinentes y no excesivos con respecto a los fines para los que fueren registrados.

d) Exactos y, si fuere necesario, tenidos al día.

e) Conservados en forma que permitiere la identificación de los interesados durante un plazo que no excediere del necesario para los fines para los cuales fueren registrados.

Artículo 6. *Clases especiales de datos.*

Los datos de carácter personal que revelaren 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, no podrán ser elaborados automáticamente a menos que el Derecho interno previere las oportunas garantías. La misma regla se aplicará a los datos de carácter personal referentes a condenas criminales.

Artículo 7. *Seguridad de los datos.*

Se adoptarán las medidas de seguridad oportunas para proteger los datos de carácter personal registrados en archivos automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, modificación o difusión no autorizados.

Artículo 8. *Garantías complementarias para el interesado.*

Toda persona deberá:

a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus fines principales, así como la identidad y la residencia habitual o el establecimiento principal del responsable del fichero.

b) Obtener en intervalos razonables y sin demoras o gastos excesivos, la confirmación de que haya en el fichero automatizado o no datos de carácter personal que le concernieren, así como la comunicación de tales datos en forma inteligible.

c) Obtener, en su caso, la rectificación de tales datos o su cancelación cuando los mismos hubieren sido elaborados en contra de las disposiciones del Derecho interno que dieren efecto a los principios fundamentales enunciados en los artículos 5 y 6 del presente Convenio.

d) Interponer recurso si no fuere estimada una petición de confirmación o, en su caso, de comunicación, rectificación o cancelación formulada a tenor de lo previsto en los apartados b) y c) del presente artículo.

Artículo 9. *Excepciones y restricciones.*

1. No se admitirá excepción alguna a lo dispuesto en los artículos 5, 6 y 8 del presente Convenio, salvo dentro de los límites definidos en el presente artículo.

2. Podrán dejarse sin efecto las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando así estuviere previsto por la ley de la Parte y constituyere una medida necesaria en una sociedad democrática.

a) Para proteger la seguridad del Estado, para la seguridad pública, para los intereses monetarios del Estado o para la represión de los delitos.

b) Para la protección del interesado y de los derechos y libertades de otros.

3. Podrán ser previstas por la ley restricciones al ejercicio de los derechos contemplados en los apartados b), c) y d) del artículo 8, en el caso de los ficheros automatizados de carácter personal utilizados a fines estadísticos o de investigación científica, cuando manifiestamente no existieren riesgos de violación de la intimidad de las personas interesadas.

Artículo 10. *Sanciones y recursos.*

Cada Parte se obliga a prever las oportunas sanciones y recursos para los casos de violación de las disposiciones del Derecho interno que dieren cumplimiento a los principios fundamentales de protección de datos enunciados en el presente capítulo.

Artículo 11. *Ampliación de la protección.*

Ninguna de las disposiciones del presente capítulo se interpretará como si limitara o afectara a la facultad de cada Parte de conceder a las personas interesadas una protección más amplia que la prevista por el presente Convenio.

CAPITULO III

De los flujos internacionales de datos

Artículo 12. *Flujos internacionales de datos de carácter personal y Derecho interno.*

1. Las disposiciones que siguen se aplicarán a las transferencias realizadas a través de las fronteras nacionales, cualquiera que fuere el soporte utilizado, de datos de carácter personal que fueren objeto de un tratamiento automatizado o reunidos con miras a someterlos a tal tratamiento.

2. Una Parte no podrá, a los sólos efectos de la protección de la intimidad, prohibir o someter a autorización especial los flujos internacionales de datos de carácter personal con destino al territorio de otra Parte.

3. No obstante, toda Parte tendrá la facultad de dejar sin efecto lo dispuesto en el apartado 2.

a) En la medida en que su legislación previere una reglamentación específica para determinadas clases de datos o de ficheros automatizados de carácter personal, por razón de la naturaleza de tales datos o ficheros, excepto si la reglamentación de la otra Parte proporcionare una protección equivalente.

b) Cuando la transferencia se hiciere desde su territorio al territorio de un Estado no contratante a través del territorio de otra Parte, con el fin de evitar que tales transferencias dieran lugar a soslayar la aplicación de la legislación de la Parte aludida al comienzo del presente apartado.

CAPITULO IV

Del mutuo auxilio

Artículo 13. *Cooperación entre las Partes.*

1. Las Partes se obligan a prestarse asistencia mutuamente para la ejecución del presente Convenio.

2. A tal efecto:

a) Cada Parte designará una o varias autoridades, cuyas denominación y dirección comunicará al Secretario General del Consejo de Europa.

b) Cada Parte que hubiere designado a varias autoridades indicará en la comunicación aludida en el apartado precedente la competencia de cada una de tales autoridades.

3. Una autoridad designada por una Parte, a instancia de una autoridad designada por otra Parte:

a) Proporcionará información sobre su Derecho y práctica administrativa en materia de protección de datos.

b) Adoptará, de conformidad con su Derecho interno y a los solos fines de la protección de la intimidad, medidas idóneas para facilitar informaciones de hecho concernientes a un tratamiento automatizado determinado efectuado en su territorio, a excepción, en todo caso, de los datos de carácter personal que fueren objeto del tratamiento.

Artículo 14. *Asistencia a los interesados residenles en el extranjero.*

1. Cada Parte prestará a toda persona que tuviere su residencia en el extranjero asistencia en lo tocante al ejercicio de los derechos reconocidos por su Derecho interno con el fin de dar cumplimiento a los principios enunciados en el artículo 8 del presente Convenio.

2. Si una tal persona residiere en el territorio de otra Parte, deberá gozar de la facultad de formular su petición por conducto de la autoridad designada por esta Parte.

3. La petición de asistencia deberá contener todas las indicaciones necesarias que hicieren referencia a los siguientes extremos, principalmente.

a) Nombre, dirección y demás elementos pertinentes que identificaren al peticionario.

b) Fichero automatizado de datos de carácter personal al que hiciere referencia la petición, o responsable de los datos.

c) Fin de la petición.

Artículo 15. *Garantías referentes a la asistencia prestada por las autoridades designadas.*

1. La autoridad designada por una Parte, que hubiere recibido informaciones de una autoridad designada por otra Parte, bien en apoyo de una petición de asistencia que la misma hubiere formulado, no podrá hacer uso de tales informaciones para fines distintos de los precisados en la petición de asistencia.

2. Cada Parte velará porque las personas que pertenecieren a la autoridad designada o que obraren en nombre de ella, estén ligadas por las oportunas obligaciones de secreto o confidencialidad con relación a tales informaciones.

3. En ningún caso estará la autoridad designada facultada, a tenor de lo previsto en el artículo 14, apartado 2, para formular peticiones de asistencia en

nombre de un interesado que residiere en el extranjero, por propia iniciativa y sin el consentimiento expreso del interesado.

Artículo 16. *Desestimación de peticiones de asistencia.*

La autoridad designada que fuere cometida de una petición de asistencia formulada a tenor de los artículos 13 ó 14 del presente Convenio no podrá negarse a estimarla más que en los siguientes casos:

a) Si la petición fuere incompatible con las competencias que en el ámbito de la protección de datos correspondieren a las autoridades habilitadas para responder.

b) Si la petición no fuere conforme con las disposiciones del presente Convenio.

c) Si la ejecución de la petición fuere incompatible con la soberanía, la seguridad o el orden público de la Parte que la hubiere designado o con los derechos y libertades fundamentales de las personas sujetas a la jurisdicción de dicha Parte.

Artículo 17. *Gastos y tramitación de la asistencia.*

1. El auxilio que las Partes se prestaren a tenor de lo dispuesto en el artículo 13, así como la asistencia que prestaren a los interesados que residieren en el extranjero, a tenor de lo previsto en el artículo 14, no devengarán gastos ni otros derechos que no fueren los correspondientes a los peritos e intérpretes. Tales gastos y derechos serán de cuenta de la Parte que hubiera designado a la autoridad que formulare la petición de asistencia.

2. El interesado no podrá ser compelido a pagar, en relación con las actuaciones evacuadas por su cuenta dentro del territorio de otra Parte, gastos y derechos que no fueren los exigibles a las personas con residencia en el territorio de dicha Parte.

3. Las demás modalidades relativas a la asistencia, en especial las que hicieren relación a las formalidades y trámites, así como las lenguas a utilizar serán convenidas directamente entre las Partes interesadas.

CAPITULO V

Del Comité Consultivo

Artículo 18. *Composición del Comité.*

1. Se constituirá un Comité Consultivo una vez que hubiere entrado en vigor el presente Convenio.

2. Toda Parte designará un representante titular y un suplente para dicho Comité. Todo Estado miembro del Consejo de Europa que no fuere Parte en el Convenio tendrá derecho a hacerse representar en el Comité por medio de un observador.

3. El Comité Consultivo podrá, por acuerdo adoptado por unanimidad, invitar a todo Estado que no fuere miembro del Consejo de Europa ni fuere parte en el Convenio, a que se haga representar en una de sus reuniones por medio de un observador.

Artículo 19. *Funciones del Comité.*

El Comité Consultivo podrá:

a) Formular propuestas con miras a facilitar o mejorar la aplicación del Convenio.

b) Formular propuestas de enmienda del presente Convenio de conformidad con el artículo 21.

c) Emitir dictamen sobre toda propuesta de enmienda del presente Convenio que le fuere sometida de conformidad con el artículo 21, apartado 3.

d) A instancia de una Parte, emitir dictamen sobre toda cuestión relativa a la aplicación del presente Convenio.

Artículo 20. *Procedimiento.*

1. El Comité Consultivo será convocado por el Secretario General del Consejo de Europa. Celebrará su primera reunión dentro de los doce meses subsiguientes a la entrada en vigor del presente Convenio. Se reunirá con posterioridad, por lo menos una vez cada dos años y, en todo caso, cada vez que un tercio de los representantes de las Partes pidiere su convocatoria.

2. La mayoría de los representantes de las Partes constituirá el quórum necesario para celebrar una reunión del Comité Consultivo.

3. Como resultado de cada una de sus reuniones, el Comité Consultivo someterá al Comité de Ministros del Consejo de Europa un informe sobre sus trabajos y sobre el funcionamiento del Convenio.

4. A reserva de las disposiciones del presente Convenio, el Comité Consultivo redactará su reglamento de régimen interior.

CAPITULO VI

De las enmiendas

Artículo 21. *Enmiendas.*

1. Podrán ser propuestas enmiendas al presente Convenio, por una Parte, por el Comité de Ministros del Consejo de Europa o por el Comité Consultivo.

2. Toda propuesta de enmienda será comunicada por el Secretario General del Consejo de Europa a los Estados miembros del Consejo de Europa y a cada Estado no miembro que se hubiere adherido o hubiere sido invitado a adherirse al presente Convenio de conformidad con lo dispuesto en el artículo 23.

3. Asimismo, toda enmienda propuesta por una Parte o por el Comité de Ministros será comunicada al Comité Consultivo, el cual someterá al Comité de Ministros su dictamen sobre la enmienda propuesta.

4. El Comité de Ministros examinará la enmienda propuesta y todo dictamen sometido por el Comité Consultivo y podrá aprobar la enmienda.

5. El texto de toda enmienda aprobada por el Comité de Ministros, de conformidad con el apartado 4 del presente artículo, será trasladado a las Partes por su aceptación.

6. Toda enmienda aprobada de conformidad con el apartado 4 del presente artículo entrará en vigor el trigésimo día después de que todas las Partes hubieren informado al Secretario General de que la han aceptado.

CAPITULO VII

Cláusulas finales

Artículo 22. *Entrada en vigor.*

1. El presente Convenio quedará abierto a la firma de los Estados miembros del Consejo de Europa. Será sometido a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación serán depositados en poder del Secretario General del Consejo de Europa.

2. El presente convenio entrará en vigor el primer día del mes subsiguiente a la expiración del plazo de tres meses que siguiere a la fecha en la cual cinco Estados miembros del Consejo de Europa hubieren expresado su consentimiento en quedar obligados por el Convenio de conformidad con lo dispuesto en el apartado precedente.

3. Para todo Estado miembro que expresare ulteriormente su consentimiento en quedar obligado por el Convenio, éste entrará en vigor el primer día del mes que siguiere a la expiración de un plazo de tres meses subsiguiente a la fecha del depósito del instrumento de ratificación, aceptación o aprobación.

Artículo 23. *Adhesión de Estados no miembros.*

1. Una vez que hubiere entrado en vigor el presente Convenio, el Comité de Ministros del Consejo de Europa podrá invitar a todo Estado no miembro del Consejo de Europa a adherirse al presente Convenio por acuerdo adoptado por la mayoría prevista en el artículo 20 d) del Estatuto del Consejo de Europa y por unanimidad de los representantes de los Estados contratantes con derecho a formar parte del Comité.

2. Para todo Estado que se adhiriere, el Convenio entrará en vigor el primer día del mes que siguiere a la expiración de un plazo de tres meses subsiguiente a la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.

Artículo 24. *Cláusula territorial.*

1. Todo Estado podrá, en el momento de la firma o en el momento del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión designar el territorio o territorios a los cuales se aplicará el presente Convenio.

2. Todo Estado podrá en todo otro momento ulterior, mediante declaración dirigida al Secretario General del Consejo de Europa, ampliar la aplicación del presente Convenio a todo otro territorio designado en la declaración. El Convenio entrará en vigor con relación a dicho territorio el primer día del mes que siguiere a la expiración de un plazo de tres meses subsiguiente a la fecha de la recepción de la declaración por el Secretario General.

3. Toda declaración hecha en virtud de los dos apartados precedentes podrá ser retirada, en lo que respecta a todo territorio designado en la declaración, mediante notificación dirigida al Secretario General. La retirada surtirá efecto el primer día del mes que siguiere a la expiración de un plazo de seis meses subsiguiente a la fecha de recepción de la notificación por el Secretario General.

Artículo 25. *Reservas.*

No se admitirá reserva alguna a las disposiciones del presente Convenio.

Artículo 26. *Denuncia.*

1. Toda Parte podrá, en todo momento, denunciar el presente Convenio por medio de notificación dirigida al Secretario General del Consejo de Europa.

2. La denuncia surtirá efecto el primer día del mes subsiguiente a la expiración de los seis meses que siguieren a la fecha de recepción de la notificación por el Secretario General.

Artículo 27. *Notificaciones.*

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo y a todo Estado que se hubiere adherido al presente Convenio:

a) Toda firma.

b) El depósito de todo instrumento de ratificación, aceptación, aprobación o adhesión.

c) Toda fecha de entrada en vigor del presente convenio de conformidad con sus artículos 22, 23 y 24.

d) Cualquier otro acto, notificación o comunicación que guarde relación con el presente convenio.

Hecho en Estrasburgo, el 28 de enero de 1981, en francés y en inglés, siendo ambos textos igualmente fehacientes, en un único ejemplar que será depositado en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa expedirá copia certificada del mismo a cada uno de los Estados miembros del Consejo de Europa y a todo Estado invitado a adherirse al presente Convenio.

ANEXO II

LEY ORGANICA 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
("B.O.E." núm. 262, de 31 de octubre de 1992)

JUAN CARLOS I.
REY DE ESPAÑA

A todos los que la presente vieren y entendieren.
Sabed: Que las Cortes Generales han aprobado, y yo
vengo en sancionar la siguiente Ley Orgánica:

Exposición de Motivos

1

La Constitución española, en su artículo 18.4, emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. La aún reciente aprobación de nuestra Constitución y, por tanto, su moderno carácter, le permitió expresamente la articulación de garantías contra la posible utilización torticera de ese fenómeno de la contemporaneidad que es la informática.

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.

Ello es así porque, hasta el presente, las fronteras de la privacidad estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona.

Uno y otro límite han desaparecido hoy: Las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos. Los más diversos datos sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado "dinero plástico", sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideológías, por poner sólo algunos ejemplos—relativos a las personas podrían ser, así, compilados y obtenidos sin dificultad. Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo deben tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que él autorice. Aún más: El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expre-

sión del honor; y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos.

Se hace preciso, pues, delimitar una nueva frontera de la intimidad y del honor, una frontera que, sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes; una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas. La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 de la Constitución, y al cumplimiento de ese objetivo responde la presente Ley.

2

Partiendo de que su finalidad es hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos, la Ley se nuclea en torno a los que convenionalmente se denominan "ficheros de datos": Es la existencia de estos ficheros y la utilización que de ellos podría hacerse la que justifica la necesidad de la nueva frontera de la intimidad y del honor.

A tal efecto, la Ley introduce el concepto de tratamiento de datos, concibiendo los ficheros desde una perspectiva dinámica; dicho en otros términos, no los entiende sólo como un mero depósito de datos, sino también, y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el perfil personal al que antes se hizo referencia.

La Ley está animada por la idea de implantar mecanismos cautelares que prevengan las violaciones de la privacidad que pudieran resultar del tratamiento de la información. A tal efecto se estructura en una parte general y otra especial.

La primera atiende a recoger los principios en los que ha cristalizado una *opinio iuris*, generada a lo largo de dos décadas, y define derechos y garantías encaminados a asegurar la observancia de tales principios generales. Alimentan esta parte general, pues, preceptos delimitadores del ámbito de aplicación de la Ley, principios reguladores de la recogida, registro y uso de datos personales y, sobre todo, garantías de la persona.

El ámbito de aplicación se define por exclusión, quedando fuera de él, por ejemplo, los datos anónimos, que constituyen información de dominio público o recogen información, con la finalidad, precisamente, de darla a conocer al público en general —como pueden ser los registros de la propiedad o mercantiles—, así como, por último, los de uso estrictamente personal. De otro lado, parece conveniente la permanencia de las regulaciones especiales que contienen ya suficientes normas de protección y que se refieren a ámbitos que revisten tal singularidad en cuanto a sus funciones y sus mecanismos de puesta al día y rectificación que aconsejan el mantenimiento de su régimen específico. Así ocurre, por ejemplo, con las regulaciones de los ficheros electorales, del Registro Civil o del Registro Central de Penados y Rebeldes; así acontece, también, con los ficheros regulados por la Ley 12/1989, de 12 de mayo, sobre función estadística pública, si bien que, en este último caso, con sujeción a la Agencia de Protección de Datos. En fin, quedan también fuera del ámbito de la norma aquellos datos que, en virtud de intereses públicos prevalentes, no deben estar sometidos a su régimen cautelar.

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 la racionalidad de la utilización de los datos. Este principio, verdaderamente cardinal, de la congruencia y la racionalidad, garantiza que los datos no puedan ser usados sino cuando lo justifique la finalidad para la que han sido recabados; su observancia es, por ello, capital para evitar la difusión incontrolada de la información que, siguiendo el mandato constitucional, se pretende limitar.

Por su parte, el principio de consentimiento, o de autodeterminación otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes. Su base está constituida por la exigencia del consentimiento consciente e informado del afectado para que la recogida de datos sea lícita; sus contornos, por otro lado, se refuerzan singularmente en los denominados "datos sensibles", como pueden ser, de una parte, la ideología o creencias religiosas -cuya privacidad está expresamente garantizada por la Constitución en su artículo 16.2— y, de otra parte, la raza, la salud y la vida sexual. La protección reforzada de estos datos viene determinada porque los primeros de entre los datos mencionados sólo serán disponibles con el consentimiento expreso y por escrito del afectado, y los segundos sólo serán susceptibles de recopilación mediando dicho consentimiento o una habilitación legal expresa, habilitación que, según exigencia de la propia Ley Orgánica, ha de fundarse en razones de interés general; en todo caso, se establece la prohibición de los ficheros creados con la exclusiva finalidad de almacenar datos personales que

expresen las mencionadas caracteristicas. En este punto, y de acuerdo con lo dispuesto en el artículo 10 de la Constitución, se atienden las exigencias y previsiones que para estos datos se contienen en el Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal, de 1981, ratificado por España.

Para la adecuada configuración, que esta Ley se propone, de la nueva garantía de la intimidad y del honor, resulta esencial la correcta regulación de la cesión de los datos almacenados. Es, en efecto, el cruce de los datos almacenados en diversas instancias o ficheros el que puede arrojar el repetidamente aludido perfil personal, cuya obtención transgrediría los límites de la privacidad. Para prevenir estos perturbadores efectos, la Ley completa el principio del consentimiento, exigiendo que, al procederse a la recogida de los datos, el afectado sea debidamente informado del uso que se les pueda dar, al objeto de que el consentimiento se preste con conocimiento cabal de su exacto alcance. Sólo las previsiones del convenio Europeo para la protección de los Derechos Fundamentales de la Persona—artículo 8.2— y del Convenio 108 del Consejo de Europa—artículo 9.2—, que se fundamentan en exigencias lógicas en toda sociedad democrática, constituyen excepciones a esta regla.

3

Las garantías de la persona son los nutrientes nucleares de la parte general, y se configuran jurídicamente como derechos subjetivos encaminados a hacer operativos los principios genéricos. Son, en efecto, los derechos de autodeterminación, de amparo, de rectificación y de cancelación los que otorgan virtualidad normativa y eficacia jurídica a los principios consagrados en la parte general, principios que, sin los derechos subjetivos ahora aludidos, no rebasarían un contenido meramente programático.

En concreto, los derechos de acceso a los datos, de rectificación y de cancelación, se constituyen como piezas centrales del sistema cautelar o preventivo instaurado por la Ley. El primero de ellos ha cobrado en nuestro país, incluso, plasmación constitucional en lo que se refiere a los datos que obran en poder de las Administraciones Públicas (artículo 105 b). En consonancia con ello queda recogido en la Ley en términos rotundos, no previéndose más excepciones que las derivadas de la puesta en peligro de bienes jurídicos en lo relativo al acceso a los datos policiales y a los precisos, para asegurar el cumplimiento de las obligaciones tributarias en lo referente a los datos de este carácter, excepciones ambas que pueden entenderse expresamente recogidas

en el propio precepto constitucional antes citado, así como en el Convenio Europeo para la protección de los Derechos Fundamentales.

4

Para la articulación de los extremos concretos que han de regir los ficheros de datos, la parte especial de la Ley comienza distinguiendo, en su Título Cuarto, entre los distintos tipos de ficheros, según sea su titularidad pública o privada. Con la pretensión de evitar una perniciosa burocratización, la Ley ha desechado el establecimiento de supuestos como la autorización previa o la inscripción constitutiva en un registro. Simultáneamente, ha establecido regímenes diferenciados para los ficheros en razón de su titularidad, toda vez que, con toda evidencia, resulta más problemático el control de los de titularidad privada que el de aquéllos de titularidad pública. En efecto, en lo relativo a estos últimos, no basta la mera voluntad del responsable del fichero sino que es precisa norma habilitante, naturalemente pública y sometida al control jurisdiccional, para crearlos y explotarlos, siendo en estos supuestos el informe previo del órgano de tutela el cauce idóneo para controlar la adecuación de la explotación a las exigencias legales y recomendar, en su caso, las medidas pertinentes.

Otras disposiciones de la parte especial que procede destacar son las atinentes a la transmisión internacional de los datos. En este punto, la Ley traspone la norma del artículo 12 del convenio 108 del Consejo de Europa, apuntando así una solución para lo que ha dado en llamarse flujo transfronterizo de datos. La protección de la integridad de la información personal se concilia, de esta suerte, con el libre flujo de los datos, que constituye una auténtica necesidad de la vida actual de la que las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional pueden ser simples botones de muestra. Se ha optado por exigir que el país de destino cuente en su ordenamiento con un sistema de protección equivalente al español, si bien permitiendo la autorización de la Agencia cuando tal sistema no exista pero se ofrezcan garantías suficientes. Con ello no sólo se cumple con una exigencia lógica, la de evitar un fallo que pueda producirse en el sistema de protección a través del flujo a países que no cuentan con garantías adecuadas, sino también con las previsiones de instrumentos internacionales como los Acuerdos de Schengen o las futuras normas comunitarias.

5

Para segurar 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.

La Agencia se caracteriza por la absoluta independencia de su Director en el ejercicio de sus funciones, independencia que trae causa, en primer lugar, de un expreso imperativo legal, pero que se garantiza, en todo caso, mediante el establecimiento de un mandato fijo que sólo puede ser acortado por un número clausus de causas de cese.

La Agencia dispondrá, además, de un órgano de apoyo definido por los caracteres de colegiación y representatividad, en el que obtendrán presencia las Cámaras que representan a la soberanía nacional, las Administraciones Públicas en cuanto titulares de ficheros objeto de la presente Ley, el sector privado, las organizaciones de usuarios y consumidores y otras personas relacionadas con las diversas funciones que cumplen los archivos informatizados.

6

El inevitable desfase que las normas de derecho positivo ofrecen respecto de las transformaciones sociales es, si cabe, más acusado en este terreno, cuya evolución tecnológica es especialmente, dinámica. Ello hace aconsejable, a la hora de normar estos campos, acudir a mecanismos jurídicos dotados de menor nivel de vinculación, susceptibles de una elaboración o modificación más rápida de lo habitual y caracterizados porque es la voluntaria aceptación de sus destinatarios la que les otorga eficacia normativa. En este línea, la Ley recoge normas de autorregulación, compatibles con las recomendaciones de la Agencia, que evitan los inconvenientes derivados de la especial rigidez de la Ley Orgánica que, por su propia naturaleza, es inidónea para un acentuado casuismo. La propia experiencia de lo ocurrido con el Convenio del Consejo de Europa, que ha tenido que ser objeto de múltiples modificaciones al socaire de las distintas innovaciones tecnológicas, de las sucesivas y diferentes aplicaciones —estadística, Seguridad Social, relaciones de empleo, datos policiales, publicidad directa o tarjetas de crédito, entre otras— o de la ampliación de los campos de utilización— servicio telefónico o correo electrónico— aconseja recurrir a las citadas normas de autorregulación. De ahí que la Ley acuda a ellas para aplicar las previsiones legales a los distintos sectores de actividad.

Tales normas serán elaboradas por iniciativa de las asociaciones y organizaciones pertinentes y serán aprobadas, sin valor reglamentario, por la Agencia, siendo precisamente la iniciativa y participación de las entidades afectadas la garantía de la virtualidad de las normas.

7

La Ley no consagra nuevos tipos delictivos, ni define supuestos de responsabilidad penal para la eventualidad de su incumplimiento. Ello obedece a que se entiende que la sede lógica para tales menesteres no es esta Ley, sino sólo el Código Penal.

Sí se atribuye, sin embargo, a la Administración la potestad sancionadora que es lógico correlato de su función de inspección del uso de los ficheros, similar a las demás inspecciones administrativas, y que se configura de distinta forma según se proyecte sobre la utilización indebida de los ficheros públicos, en cuyo caso procederá la oportuna responsabilidad disciplinaria, o sobre los privados, para cuyo supuesto se prevén sanciones pecuniarias.

De acuerdo con la práctica usual, la Ley se limita a tipificar, de conformidad con lo requerido por la jurisprudencia constitucional y ordinaria, unos supuestos genéricos de responsabilidad administrativa, recogiendo una gradación de infracciones que sigue la habitual distinción entre leves, graves y muy graves, y que toma como criterio básico el de los bienes jurídicos emanados. Las sanciones, a su vez, difieren, según que los ficheros indebidamente utilizados sean públicos o privados: en el primer caso, procederá la responsabilidad disciplinaria, sin perjuicio de la intervención del Defensor del Pueblo; para el segundo, se prevén sanciones pecuniarias; en todo caso, se articula la posibilidad en los supuestos, constitutivos de infracción muy grave, de cesión ilícita de datos o de cualquier otro atentado contra los derechos de los afectados que revista gravedad, de inmovilizar los ficheros.

8

Finalmente, la Ley estipula un período transitorio que se justifica por la necesidad de ajustar la utilización de los ficheros existentes a las disposiciones legales.

Pasado este período transitorio, y una vez en vigor la Ley, podrá muy bien decirse, una vez más, que el desarrollo legislativo de un precepto constitucional se traduce en una protección reforzada de los derechos fundamenta-

les del ciudadano. En este caso, al desarrollar legislativamente el mandato constitucional de limitar el uso de la informática, se está estableciendo un nuevo y más consistente derecho a la privacidad de las personas.

TITULO PRIMERO

Disposiciones generales

Artículo 1. *Objeto.*

La presente Ley Orgánica, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

Artículo 2. *Ambito de aplicación.*

1. La presente Ley será de aplicación a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley no será de aplicación:

a) A los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general.

b) A los ficheros mantenidos por personas físicas con fines exclusivamente personales.

c) A los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales.

d) A los ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en períodicos o repertorios oficiales.

e) A los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros, sin perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos.

3. Se regirán por sus disposiciones específicas:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los sometidos a la normativa sobre protección de materias clasificadas.

c) Los derivados del Registro Civil y del Registro Central de Penados y Rebeldes.

d) Los que sirvan a fines exclusivamente estadísticos y estén amparados por la Ley 12/1989, de 9 de mayo, de la función estadística pública, sin perjuicio de lo dispuesto en el artículo 36.

e) Los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el artículo 68 de la Ley 17/1989, de 19 de julio, Reguladora del Régimen del Personal Militar Profesional.

Artículo 3. *Definiciones.*

A los efectos de la presente Ley se entenderá por:

a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero automatizado: Todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: Operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero: Persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable.

TITULO II

Principios de la protección de datos

Artículo 4. *Calidad de los datos.*

1. Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido.

En su clasificación sólo podrán utilizarse criterios que no se presten a prácticas ilícitas.

2. Los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para finalidades distintas de aquéllas para las que los datos hubieran sido recogidos.

3. Dichos datos serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 15.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos sus valores históricos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Serán almacenados de forma que permitan el ejercicio del derecho de acceso por parte del afectado.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. *Derecho de información en la recogida de datos.*

1. Los afectados a los que se soliciten datos personales deberán 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.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será la necesaria la información a que se refiere el apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Artículo 6. *Consentimiento del afectado.*

1. El tratamiento automatizádo de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

Artículo 7. *Datos especialmente protegidos.*

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento automatizado los datos de carácter personal que revelen la ideología, religión y creencias.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados automatizadamente y cedidos cuando por razones de interés general así lo disponga una Ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideologia, religión, creencias, origen racial o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros automatizados

de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Artículo 8. *Datos relativos a la salud.*

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento automatizado de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en los artículos 8, 10, 2 y 61 de la Ley 14/1986, de 25 de abril, General de Sanidad; 85.5, 96 y 98 de la Ley 25/1990, de 20 de diciembre, del Medicamento; 2, 3 y 4 de la Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de Salud Pública y demás Leyes sanitarias.

Articulo 9. *Seguridad de los datos*

1. El responsable del fichero deberá 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 automatizados 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 automatizados y las personas que intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. *Deber de secreto.*

El responsable del fichero automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo.

Artículo 11. *Cesión de datos.*

1. Los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando una Ley prevea otra cosa.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros. En este caso, la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tienen atribuidas.

e) Cuando la cesión se produzca entre las Administraciones Públicas en los supuestos previstos en el artículo 19.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado o para realizar los estudios epidemiológicos en los términos establecidos en el artículo 8 de la Ley 14/1986, de 25 de abril, General de Sanidad.

3. Será nulo el consentimiento cuando no recaiga sobre un cesionario determinado o determinable, o si no constase con claridad la malidad de la cesión que se consiente.

4. El consentimiento para la cesión de datos de carácter personal tiene también un carácter de revocable.

5. El cesionario de los datos de carácter personal se obliga, por el sólo hecho de la cesión, a la observancia de las disposiciones de la presente Ley.

6. Si la cesión se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

TITULO III

Derechos de las personas

Artículo 12. *Impugnación de valoraciones basadas exclusívamente en datos automatizados.*

El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad.

Artículo 13. *Derecho de información.*

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de ficheros automatizados de datos de carácter personal, sus finalidades y la identidad del responsable del fichero. El Registro general será de consulta pública y gratuita.

Artículo 14. *Derecho de acceso.*

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 doce meses, salvo que al afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Artículo 15. *Derecho de rectificación y cancelación.*

1. 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.

2. Los datos de carácter personal que resulten inexactos o incompletos serán rectificados y cancelados en su caso.

3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario.

4. La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos.

5. 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 fichero y el afectado.

Artículo 16. *Procedimiento de acceso.*

1. El procedimiento para ejercitar el derecho de acceso, así como el de rectificación y cancelación será establecido reglamentariamente.

2. No se exigirá contraprestación alguna por la rectificación o cancelación de los datos de carácter personal inexactos.

Artículo 17. *Tutela de los derechos y derechos de indemnización.*

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los afectados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

3. Los afectados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable del fichero, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

4. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

5. En el caso de los ficheros de titularidad privada la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TITULO IV

Disposiciones sectoriales

CAPITULO PRIMERO

Ficheros de titularidad pública

Artículo 18. *Creación, modificación o supresión.*

1. La creación, modilcación 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.

2. Las disposiciiones de creación o de modificación de los 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.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero automatizado y la descripción de los tipos de datos de carácter personal que, en su caso, se prevean.

e) Las cesiones de datos de carácter personal que, en su caso, se prevean.

f) Los órganos de la Administración responsables del fichero automatizado.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación y cancelación.

3. En las disposiciones que se dicten para la supresión de los ficheros automatizados se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 19. *Cesión de datos entre Administraciones Públicas.*

1. 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.

2. Podrán, en todo caso, ser objeto de cesión los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2.b) la cesión de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una Ley prevea otra cosa.

Artículo 20. *Ficheros de las Fuerzas y Cuerpos de Seguridad.*

1. Los ficheros automatizados creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento automatizado para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías, en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusívamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judi-

cial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 21. *Excepciones a los derechos de acceso, rectificación y cancelación.*

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 la 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 automatizados mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones Tributarias Autonómicas, quien deberá asegurarse de la procedencia o improcedencia de la denegación.

Artículo 22. *Otras excepciones a los derechos de los afectados.*

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 cumplimiento 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 artículo 14 y en el apartado 1 del artículo 15 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos concedan 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.

CAPITULO II

Ficheros de titularidad privada

Artículo 23. *Creación.*

Podrán crearse ficheros automatizados de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimo de la persona, empresa o entidad titular y se respeten las garantías que esta ley establece para la protección de las personas.

Artículo 24. *Notificación e inscripción registral.*

1. Toda persona o entidad que proceda a la creación de ficheros automatizados 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 y las cesiones de datos de carácter personal que contiene las medidas de seguridad y las cesiones de datos de carácter personal que se prevean realizar.

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 automatizado 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.

Artículo 25. *Comunicación de la cesión de datos.*

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando asimismo la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d) y e), y 6 del artículo 11 ni cuando la cesión venga impuesta por Ley.

Artículo 26. *Datos sobre abonados a servicios de telecomunicación.*

Los números de los teléfonos y demás servicios de telecomunicación, junto con otros datos complementarios, podrán figurar en los repertorios de abonados de acceso al público, pero el afectado podrá exigir su exclusión.

Artículo 27. *Prestación de servicios de tratamiento automatizado de datos de carácter personal.*

1. Quienes, por cuenta de terceros, presten servicios de tratamiento automatizado de datos de carácter personal no podrán aplicar o utilizar los obtenidos con un fin distinto al que figure en el contrato de servicios, ni cederlos, ni siquiera para su conservación, a otras personas.

2. Una vez cumplida la prestación contractual, los datos de carácter personal tratados deberán ser destruidos, salvo que medie autorización expresa de aquél por cuenta de quien se prestan tales servicios, porque razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrán almacenar con las debidas condiciones de seguridad por un período de cinco años.

Artículo 28. *Prestación de servicios de información sobre solvencia patrimonial y crédito.*

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar automatizadamente datos de carácter personal obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento. Podrán tratarse, igualmente, datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quiena actúe por su cuenta o interés. En estos casos se notificará a los

afectados respecto de los que hayan registrado datos de carácter personal en ficheros automatizados, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

2. Cuando el afectado lo solicite, el responsable del fichero le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección del cesionario.

3. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los afectados y que no se refieran, cuando sean adversos, a más de seis años.

Artículo 29. *Ficheros con fines de publicidad.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad o venta directa y otras actividades análogas, utilizarán listas tratadas automáticamente de nombres y direcciones u otros datos personales, cuando los mismos figuren en documentos accesibles al público o cuando hayan sido facilitados por los propios afectados u obtenidos con su consentimiento.

2. Los afectados tendrán derecho a conocer el origen de sus datos de carácter personal, así como a ser dados de baja de forma inmediata del fichero automatizado, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 30. *Ficheros relativos a encuestas o investigaciones.*

1. Sólo se utilizarán de forma automatizada datos de carácter personal en las encuestas de opinión, trabajos de prospección de mercados, investigación científica o médica y actividades análogas, si el afectado hubiera prestado libremente su consentimiento a tal efecto.

2. Los datos de carácter personal tratados automáticamente con ocasión de tales actividades no podrán ser utilizados con finalidad distinta ni cedidos de forma que puedan ser puestos en relación con una persona concreta.

Artículo 31. *Códigos tipo.*

1. Mediante acuerdos sectoriales o decisiones de empresa, los responsables de ficheros de titularidad privada podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto de los principios y disposiciones de la presente Ley y sus normas de desarrollo.

Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporaran directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos, que podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TITULO V

Movimiento internacional de datos

Artículo 32. *Norma general.*

No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos que sólo podrá otorgarla si se obtienen garantías adecuadas.

Artículo 33. *Excepciones.*

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial Internaclonal,

c) Cuando la misma tenga por objeto el intercambio de datos de carácter médico entre facultativos o instituciones sanitarias y así lo exija el tratamiento del afectado o la investigación epidemiológica de enfermedades o brotes epidémicos.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

TITULO VI

Agencia de Protección de Datos

Artículo 34. *Naturaleza y régimen jurídico.*

1. Se crea la Agencia de Protección de Datos.

2. 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. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio que será aprobado por el Gobierno, así como por aquellas disposiciones que le sean aplicables en virtud del artículo 6.5 de la Ley General Presupuestaria.

3. En el ejercicio de sus funciones públicas, y en defecto de lo que dispongan la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley de Procedimiento Administrativo. En sus adquisiciones patrimoniales y contratación estará sujeta al Derecho privado.

4. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones Públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

5. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.

b) Los bienes y valores que constituyan su patrimonio. así como los productos y rentas del mismo.

c) Cualesquiera otros que legalmente puedan serle atribuidos.

6. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 35. *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.

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.

Artículo 36. *Funciones.*

Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la presente Ley.

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas .

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento automatizado de los datos de carácter personal.

f) Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros, cuando no se ajusten a las disposiciones de la presente Ley.

g) Ejercer la potestad sancionadora en los términos previstos por el título VII de la presente Ley.

h) Informar con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros automatizados de dato, con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

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.

m) Velar por el cumplimiento de las disposiciones que la Ley de la función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 45.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Artículo 37. *Consejo Consultivo.*

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

Un Diputado, propuesto por el Congreso de los Diputados.

Un Senador, propuesto por la correspondiente Cámara.

Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.

Un miembro de la Real Academia de la Historia, propuesto por la misma.

Un experto en la materia, propuesto por el Consejo Superior de Universidades .

Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

Un representante de las Comunidades Autónomas, cuya propuesta se realizará a través del procedimiento que se establezca en las disposiciones de desarrollo de esta Ley.

Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 38. *El Registro General de Protección de Datos.*

1. Se crea el Registro General de Protección de Datos como órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros automatizados de que sean titulares las Administraciones Públicas.

b) Los ficheros automatizados de titularidad privada.

c) Las autorizaciones a que se refiere la presente Ley.

d) Los códigos tipo a que se refiere el artículo 31 de la presente Ley.

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación y cancelación.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 39. *Potestad de inspección.*

1. La Agencia de Protección de Datos podrá inspeccionar los ficheros a que hace referencia la presente Ley recabando cuantas informaciones precise para el cumplimiento de sus cometidos.

A tal efecto, podrá solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior, tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 40. *Organos correspondientes de las Comunidades Autónomas.*

1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 36, 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 45 y 48, en relación con sus específicas competencias, serán ejercidas, cuando afecten a ficheros automatizados de datos de carácter personal creados o gestionados por las Comunidades Autónomas por

los órganos correspondientes por cada Comunidad, a los que se garantizará plena independencia y objetividad en el ejercicio de su cometido.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros públicos para el ejercicio de las competencias que se les reconoce sobre los mismos, respecto de los archivos informatizados de datos personales cuyos titulares sean los órganos de las respectivas Comunidades Autónomas o de sus Territorios Históricos.

3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios y procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 41. *Ficheros de las Comunidades Autónomas en materias de su exclusiva competencia.*

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero automatizado de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia, podrá requerir a la Administración correspondiente para que adopte las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.

2. Si la Administración Pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TITULO VII

Infracciones y sanciones

Artículo 42. *Responsables.*

1. Los responsables de los ficheros estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando se trate de ficheros de los que sean responsables las Administraciones Públicas se estará, en cuanto al procedimiento y a las sanciones a lo dispuesto en el artículo 45, apartado 2.

Artículo 43. *Tipos de infraciones.*

1. Las infracciones se calificarán como leves, graves o muy graves.

Son infracciones leves:

a) No proceder, de oficio o a solicitud de las personas o instituciones legalmente habilitadas para ello, a la rectificación o cancelación de los errores, lagunas o inexactitudes de carácter formal de los ficheros.

b) No cumplir las instrucciones dictadas por el Director de la Agencia de Protección de Datos. o no proporcionar la información que éste solicite en relación a aspectos no sustantivos de la protección de datos.

c) No conservar actualizados los datos de carácter personal que se mantengan en ficheros automatizados.

d) Cualquiera otra que afecte a cuestiones meramente formales o documentales y que no constituya infracción grave o muy grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros automatizados de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.

b) Proceder a la creación de ficheros automatizados de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de caráeter personal sin recabar el consentimiento expreso de las personas afectadas, en los easos en que éste sea exigible, o sin proporcionarles la información que señala el artículo 5 de la presente Ley.

d) Tratar de forma automatizada los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidas en

la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculizaeión del ejercicio del derecho de acceso y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneraeión del deber de guardar secreto, cuando no constituya infracción muy grave.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal fuera de los casos en que estén permitidas.

c) Recabar y tratar de forma automatizada los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar de forma automatizada los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una Ley o el afectado no haya consentido expresamente o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos automatizados de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia, temporal o definitiva, de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar de forma automatizada los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7.

Artículo 44. *Tipos de sanciones.*

1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.

2. Las infracciones graves serán sancionadas con multa de 10.000.001 pesetas a 50.000.000 de pesetas.

3. Las infracciones muy graves serán sancionadas con multa de 50.000.001 pesetas a 100.000.000 de pesetas.

4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad y a la reincidencia.

5. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 45. *Infracciones de las Adminislraciones Públicas.*

1. Cuando las infracciones a que se refiere el artículo 43 fuesen cometidas en ficheros de los que sean responsables las 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.

Artículo 46. *Prescripción.*

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causa no imputable al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas grves a los dos años y la impuestas por faltas leves al año.

5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquél en que adquiera firmeza la resolución por la que se impone la sanción.

6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo esta paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 47. *Plocedimiento sancionador.*

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente título.

2. Contra las resoluciones de la Agencia de Protección de Datos, u órgano correspondiente de la Comunidad Autónoma, procederá recurso contencioso-administrativo

Artículo 48. *Potestad de inmovilización de ficheros.*

En los supuestos. constitutivos de infracción mu grave de utilización o cesión ilicita 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 automatizados de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los delitos. Si el requerimiento fuera desatendido la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros automatizados a los solos efectos de restaurar los derechos de las personas afectadas.

Disposición adicional primera. *Exclusión de la aplicación de los Títulos VI y VII.*

Lo dispuesto en los Títulos VI y VII no es de aplicación a los ficheros automatizados de los que sean titulares las Cortes Generales, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo General del Poder Judicial y el Tribunal Constitucional.

Disposición adicional segunda. *Ficheros existentes con anterioridad a la entrada en vigor de la Ley.*

1. Dentro del año siguiente a la entrada en vigor de la presente Ley Orgánica deberán ser comunicados a la Agencia de Protección de Datos los ficheros y tratamientos automatizados de datos de carácter personal existentes con anterioridad y comprendidos dentro de su ámbito de aplicación.

2. Dentro del año siguiente a la entrada en vigor de la presente Ley Orgánica, las Administraciones Públicas responsables de ficheros automatizados ya existentes deberán adoptar una disposición de regulación del fichero o adaptar la que existiera.

Disposición adicional tercera. *Competencias del Defensor del Pueblo.*

Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

Disposición transitoria única. *Adaptaciones complejas a lo establecido en la Ley.*

Cuando la adaptación de los ficheros automatizados a los principios y derechos establecidos en la presente Ley requiera la adopción de medidas técnicas complejas o el tratamiento de un gran volumen de datos, tales adaptaciones y tratamientos deberán realizarse en el plazo de un año desde la entrada en vigor de la Ley, sin perjuicio del cumplimiento, en todo lo demás, de las disposiciones de la misma.

Disposición derogatoria única. *Derogación de la disposición transitoria primera de la Ley Orgánica 1/1992.*

Queda derogada la disposición transitoria primera de 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.

Disposición final primera. *Habilitación de desarrollo reglamentario.*

El Gobierno dictará las disposiciones necesarias para la aplicación y desarrollo de la presente Ley, y para regular la estructura orgánica de la Agencia de Protección de Datos.

Disposición final segunda. *Extensión de la aplicación de la Ley a ficheros convencionales.*

El Gobierno, previo informe del Director de la Agencia de Protección de Datos, podrá extender la aplicación de la presente Ley, con las modificaciones y adaptaciones que fuesen necesarias, a los ficheros que contengan datos almacenados en forma convencional y que no hayan sido sometidos todavía o no estén destinados a ser sometidos a tratamiento automatizado.

Disposición final tercera. *Preceptos con carácter de Ley ordinaria.*

Los artículos 18, 19, 23, 26, 27, 28, 29, 30, 31, los Títulos VI y VII, las disposiciones adicionales primera y segunda y la disposición final primera tienen carácter de Ley ordinaria.

Disposición final cuarta. *Entrada en vigor.*

La presente Lev Orgánica entrará en vigor a los tres meses de su publicación en el "Boletín Oficial del Estado".

Madrid, 29 de octubre de 1992.

JUAN CARLOS R.

El Presidente del Gobierno.
FELIPE GONZALEZ MARQUEZ

ANEXO III

REAL DECRETO 428/1993, de 26 de marzo,
por el que se aprueba el Estatuto de la Agencia de Protección de Datos.
("B.O.E." de 4 de mayo de 1993)

El título VI de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, ha configurado la Agencia de Protección de Datos como el ente independiente que debe garantizar el cumplimiento de las previsiones y mandatos en ella establecidos.

Algunos aspectos de dicho ente han sido objeto de regulación en la propia Ley que, no obstante, no ha agotado la materia y ha encomendado al Gobierno la regulación de la estructura orgánica y la aprobación del Estatuto de la Agencia de Protección de Datos.

Por medio de la presente disposición se procede a cumplimentar el doble mandato integrando la estructura del ente en su Estatuto propio.

En su virtud, a propuesta de los Ministros de Justicia y para las Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 26 de marzo de 1993,

DISPONGO:

Artículo único.

De conformidad con lo dispuesto en el artículo 34.2 y en la disposición final primera de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, se aprueba el Estatuto de la Agencia de Protección de Datos, cuyo texto se inserta a continuación.

Disposición adicional única.

Por el Ministerio de Economía y Hacienda se habilitarán los créditos necesarios para la instalación y funcionamiento de la Agencia de Protección de Datos, en tanto no sea aprobado el primer presupuesto de gastos e ingresos de la misma.

Disposición final única.

El presente Real Decreto entrará en vigor a los veinte días de su publicación en el "Boletín Oficial del Estado".

Dado en Madrid a 26 de marzo de 1993.

JUAN CARLOS R.

El Ministro de Relaciones con las Cortes
y de la Secretaría del Gobierno.

VIRGILIO ZAPATERO GOMEZ

ESTATUTO DE LA AGENCIA DE PROTECCION DE DATOS

CAPITULO PRIMERO

Disposiciones generales

Artículo 1. *La Agencia de Protección de Datos.*

1. La Agencia de Protección de Datos es un ente de Derecho público de los previstos en el artículo 6, apartado 5, del texto refundido de la Ley General Presupuestaria, aprobado por Real Decreto legislativo 1091/1988, de 23 de septiembre, que tiene por objeto la garantía del cumplimiento y aplicación de las previsiones contenidas en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

2. 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.

Artículo 2. *Régimen jurídico.*

1. La Agencia de Protección de Datos goza de personalidad jurídica propia y plena capacidad pública y privada.

2. La Agencia de Protección de Datos se regirá por las disposiciones legales y reglamentarias siguientes:

a) El título VI de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

b) El presente Estatuto y las demás disposiciones de desarrollo de la Ley Orgánica 5/1992.

c) En defecto de las anteriores, y para el ejercicio de sus funciones públicas, las normas de procedimiento contenidas en la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

d) Los preceptos de la Ley General Presupuestaria, texto refundido aprobado por Real Decreto legislativo 1091/1988, de 23 de septiembre, que resulten de aplicación.

e) Cuantas otras disposiciones resulten de aplicación.

3. La Agencia ejercerá sus funciones por medio del Director, a cuyo efecto los actos del Director se consideran actos de la Agencia.

4. Los actos dictados por el Director en el ejercicio de las funciones públicas de la Agencia agotan la vía administrativa. Contra ellos se podrán interponer los recursos contencioso-administrativos que resulten procedentes.

CAPITULO II

Funciones de la Agencia de Protección de Datos

Artículo 3. *Funciones.*

1. Corresponde a la Agencia de Protección de Datos ejercer las funciones que le atribuye el artículo 36 de la Ley Orgánica 5/1992.

2. A este efecto la Agencia de Protección de Datos podrá dirigirse directamente a los titulares y responsables de cualesquiera ficheros de datos de carácter personal.

Artículo 4. *Relaciones con los afectados.*

1. La Agencia de Protección de Datos informará a las personas de los derechos que la Ley les reconoce en relación con el tratamiento automatizado de sus datos de carácter personal y a tal efecto podrá promover campañas de difusión, valiéndose de los medios de comunicación social.

2. La Agencia atenderá las peticiones que le dirijan los afectados y resolverá las reclamaciones formuladas por los mismos, sin perjuicio de las vías de recurso procedentes.

Artículo 5. *Cooperación en la elaboración y aplicación de las normas.*

La Agencia de Protección de Datos colaborará con los órganos competentes en lo que respecta al desarrollo normativo y aplicación de las normas que incidan en materia propia de la Ley Orgánica 5/1992, y a tal efecto:

a) Informará preceptivamente los proyectos de disposiciones generales de desarrollo de la Ley Orgánica.

b) Informará preceptivamente cualesquiera proyectos de ley o reglamento que incidan en la materia propia de la Ley Orgánica.

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.

Artículo 6. *Ficheros estadísticos.*

La Agencia de Protección de Datos ejercerá el control de la observancia de lo dispuesto en los artículos 4, 7 y 10 a 22 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, y en especial:

a) Informará con carácter preceptivo el contenido y formato de los cuestionarios, hojas censuales y otros documentos de recogida de datos con fines estadisticos.

b) Dictaminará sobre los procesos de recogida y tratamiento automatizado de los datos personales a efectos estadisticos.

c) Informará sobre los proyectos de ley por ios que se exijan datos con carácter obligatorio y su adecuación a lo dispuesto en el articulo 7 de la Ley de la Función Estadistica Pública.

d) Dictaminará sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadisticos.

Artículo 7. *Publicidad de los ficheros automatizados.*

La Agencia de Protección de Datos velará por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, a cuyo efecto publicar y difundirá un catálogo anual de los ficheros inscritos en el Registro General de Protección de Datos, con expresión de la información que al amparo de lo dispuesto en el articulo 36, j), de la Ley Orgánica 5/1992, determine el Director.

Artículo 8. *Memoria anual.*

1. La Agencia de Protección de Datos redactará una Memoria anual sobre la aplicación de la Ley Orgánica 5/1992, y de las demás disposiciones legales y reglamentarias sobre protección de datos, la cual comprenderá, además de la información necesaria sobre ei funcionamiento de la Agencia:

a) Una relación de los códigos tipo depositados e inscritos en el Registro General de Protección de Datos.

b) Un análisis de las tendencias legislativas, jurisprudenciales y doctrinales de los distintos países en materia de protección de datos.

c) Un análisis y una valoración de los problemas de la protección de datos a escala nacional.

2. La Memoria anual será remitida por el Director al Ministro de Justicia, para su ulterior envío a las Cortes Generales.

Artículo 9. *Relaciones internacionales.*

1. Corresponde a la Agencia de Protección de Datos la cooperación con organismos internacionales y órganos de las Comunidades Europeas en materia de protección de datos.

2. 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 tratamieno automatizado de los datos de carácter personal a los efectos previstos en el artículo 13 del Convenio.

Artículo 10. *Sistema de Información Schengen.*

1. La Agencia de Protección de Datos ejercerá el control de los datos de carácter personal introducidos en la parte nacional española de la base de datos del Sistema de Información Schengen (SIS).

2. El Director de la Agencia designará dos representantes para la autoridad de control común de protección de datos del Sistema de Información Schengen.

CAPÍTULO III

Organos de la Agencia de Protección e Datos

Sección 1.a

Estructura orgánica de la Agencia de Protección de Datos

Artículo 11. *Estructura orgánica.*

La Agencia de Protección de Datos se estructura en los siguientes órganos:

1. El Director de la Agencia de Protección de Datos.

2. El Consejo Consultivo.

3. El Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General, como órganos jerárquicamente dependientes del Director de la Agencia.

Sección 2.a

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 soliciten 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.

Artícuio 13. *Funciones de gestión.*

1. Corresponde asimismo al Director de la Agencia de Protección de Datos:

a) Adjudicar y formalizar los contratos que requiera la gestión de la Agencia y vigilar su cumplimiento y ejecución.

b) Aprobar gastos y ordenar pagos, dentro de los límites de los créditos del presupuesto de gastos de la Agencia.

c) Ejercer el control económico-financiero de la Agencia.

d) Programar la gestión de la Agencia.

e) Elaborar el anteptoyecto de presupuesto de la Agencia.

f) Proponer la relación de puestos de trabajo de la Agencia.

g) Aprobar la Memoria anual de la Agencia.

h) Ordenar la convocatoria de las reuniones del Consejo Consultivo.

2. El Director podrá delegar en el Secretario general el ejercicio de las funciones a que se refieren las letras a), b), d), e) y f) del apartado anterior.

Artículo 14. *Nombramiento y mandato.*

1. El Director de la Agencia de Protección de Datos será nombrado por el Gobierno, mediante Real Decreto, a propuesta del Ministro de Justicia, de entre los miembros del Consejo Consultivo.

2. El Director de la Agencia de Protección de Datos gozará de los mismos honores y tratamiento que los Subsecretarios.

3. El mandato del Director de la Agencia de Protección de Datos tendrá una duración de cuatro años contados desde su nombramiento y sólo cesara por las causas previstas en el artículo 15 del presente Estatuto.

Artículo 15. *Cese y separación.*

1. El Director de la Agencia de Protección de Datos cesará en el desempeño de su cargo por la expiración de su mandado o, con anterioridad, a petición propia.

2. El Gobierno sólo podrá acordar la separación del Director de la Agencia de Protección de Datos antes de que hubiera expirado el plazo de su mandato en los casos siguientes:

a) Incumplimiento grave de las obligaciones del cargo.

b) Incapacidad sobrevenida para el ejercicio de sus funciones.

c) Incompatibilidad.

d) Condena por delito doloso.

La separación se acordará por el Gobierno mediante Real Decreto a propuesta del Ministro de Justicia, previa instrucción de expediente, en el cual serán oídos los restantes miembros del Consejo Consultivo.

3. El cargo de Director de la Agencia de Protección de Datos está sujeto a las incompatibilidades que para los altos cargos prevé la Ley 25/1983, de 26 de diciembre.

Artículo 16. *Independencia.*

1. El Director de la Agencia de Protección de Datos desempeñará su cargo con dedicación absoluta, plena independencia y total objetividad.

2. El Director no estará sujeto a mandato imperativo, ni recibirá instrucciones de autoridad alguna.

Artículo 17. *Remuneración.*

1. El Director de la Agencia de Protección de Datos percibirá la remuneración que en los Presupuestos Generales del Estado tengan asignada los subsecretarios.

2. La remuneración será incompatible con la percepción de pensiones de derechos pasivos o de cualquier régimen de Seguridad Social público y obligatorio, quedando en suspenso dichas percepciones durante el plazo de mandato.

Sección 3.a

El Consejo Consultivo

Artículo 18. *El Consejo Consultivo.*

1. El Consejo Consultivo de la Agencia de Protección de Datos, establecido por el artículo 37 de la Ley Orgánica 5/1992, de 29 de octubre, es un órgano colegiado de asesoramiento del Director de la Agencia de Protección de Datos.

2. El Consejo Consultivo emitirá informe en todas las cuestiones que le someta el Director de la Agencia de Protección de Datos y podrá formular propuestas en temas relacionados con las materias de competencia de ésta.

Artículo 19. *Propuesta y nombramiento.*

1. Los miembros del Consejo Consultivo serán propuestos en la forma siguiente:

a) El Congreso de los Diputados propondrá, como Vocal, a un Diputado.

b) El Senado propondrá, como Vocal, a un Senador.

c) El Ministro de Justicia propondrá al Vocal de la Administración General del Estado.

d) Las Comunidades Autónomas decidirán, mediante acuerdo adoptado por mayoría simple, el Vocal a proponer.

e) La Federación Española de Municipios y Provincias propondrá al Vocal de la Administración Local.

f) La Real Academia de la Historia propondrá, como Vocal, a un miembro de la Corporación.

g) El Consejo de Universidades propondrá a un Vocal experto en la materia de entre los cuerpos docentes de enseñanza superior e investigadores con acreditado conocimiento en el tratamiento automatizado de datos.

h) El Consejo de Consumidores y Usuarios propondrá, mediante terna, al Vocal de los usuarios y consumidores.

i) El Consejo Superior de Cámaras de Comercio, Industria y Navegación propondrá, mediante terna, al Vocal del sector de ficheros privados.

2. Las propuestas serán elevadas al Gobierno por conducto del Ministro de Justicia.

3. Los miembros del Consejo Consultivo serán nombrados y, en su caso, cesados por el Gobierno.

Artículo 20. *Plazo y vacantes.*

1. Los miembros del Consejo Consultivo desempeñarán su cargo durante cuatro años.

2. Se exceptúan de lo establecido en el apartado anterior los siguientes supuestos:

a) Nombramiento del Vocal como Director de la Agencia de Protección de Datos.

b) Renuncia anticipada del Vocal.

c) Pérdida de la condición que habilitó al Vocal para ser propuesto, en los supuestos previstos en las letras a), b), f) y g) del apartado 1 del artículo anterior.

d) Propuesta de cese emanada de las instituciones, órganos, corporaciones u organizaciones a las que se refiere el artículo anterior.

3. Las vacantes que se produzcan en el Consejo Consultivo antes de expirar el plazo a que se refiere el apartado 1 deberán ser cubiertas dentro del mes siguiente a la fecha en que la vacante se hubiera producido, por el procedimiento previsto en el artículo anterior y por el tiempo que reste para completar el mandato de quien causó la vacante a cubrir.

4. Los miembros del Consejo Consultivo no percibirán retribución alguna, sin perjuicio del abono de los gastos, debidamente justificados, que les ocasione el ejercicio de su función.

Artículo 21. *Renovación del Consejo Consultivo.*

1. Antes de finalizar el mandato de los miembros del Consejo Consultivo, el Gobierno, por conducto del Ministro de Justicia, requerirá a las instituciones,

órganos, corporaciones y organizaciones a que se refiere el artículo 19 del presente Estatuto, a fin de que le comuniquen los nombres de las personas que propongan para un nuevo mandato en el Consejo Consultivo, lo que deberá efectuarse dentro del mes siguiente a la formulación del referido requerimiento.

2. Una vez transcurrido el plazo señalado para cumplimentar el requerimiento, el Gobierno procederá, sin más tramites, a nombrar como miembros del Consejo Consultivo a los propuestos, quienes tomarán posesión de su condición en la misma fecha en que expire el antenor mandato de los miembros del Consejo.

Artículo 22. *Funcionamiento.*

1. En defecto de disposiciones específicas del presente Estatuto, el Consejo Consultivo ajustará su actuación, en lo que le sea de aplicación, a las disposiciones del capítulo II del título II de la Ley 30/1992, de 26 de noviembre, de Régimen Juridico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. El Consejo Consultivo adoptará sus acuerdos en sesión plenaria.

3. Actuará como presidente del Consejo Consultivo el Director de la Agencia de Protección de Datos.

4. Actuará como secretario del Consejo Consultivo, con voz y sin voto, el titular de la Secretaria General de la Agencia de Protección de Datos. En caso de vacante, ausencia o enfermedad, actuará de secretario un funcionario adscrito a la Secretaria General designado por el Director de la Agencia a tal efecto.

5. El Consejo Consultivo se reunirá cuando así lo decida el Director de la Agencia que, en todo caso, lo convocará una vez cada seis meses. También se reunirá cuando asi lo solicite la mayoria de sus miembros.

6. El Secretario convocará las reuniones del Consejo Consultivo, de orden del Director de la Agencia, y trasladará la convocatoria a los miembros del Consejo.

7. El Consejo Consultivo quedará válidamente constituido, en primera convocatoria, si están presentes el presidente, el secretario y la mitad de los miembros del Consejo, y, en segunda convocatoria, si están presentes el presidente, el secretario y la tercera parte de los miembros del Consejo.

Sección 4.a

El Registro General de Protección de Datos

Artículo 23. *El Registro General de Protección de Datos.*

El Registro General de Protección de Datos es el órgano de la Agencia de Protección de Datos al que corresponde velar por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos regulados en los artículos 13 a 15 de la Ley Orgánica 5/1992, de 29 de octubre.

Artículo 24. *Ficheros inscribibles.*

1. Serán objeto de inscripción en el Registro los ficheros automatizados que contengan datos personales y de los cuales sean titulares:

a) La Administración General del Estado.

b) Las entidades y organismos de la Seguridad.

c) Los organismos autónomos del Estado, cualquiera que sea su clasificación.

d) Las sociedades estatales y entes del sector público a que se refiere el artículo 6 de la Ley General Presupuestaria.

e) Las Administraciones de las Comunidades Autónomas y de sus Territorios Históricos, así como sus entes y organismos dependientes, sin perjuicio de que se inscriban además en los registros a que se refiere el artículo 40.2 de la Ley Orgánica 5/1992.

f) Las entidades que integran la Administración Local y los entes y organismos dependientes de la misma.

g) Cualesquiera otras personas jurídico-públicas, así como las personas privadas, físicas o jurídicas.

2. En los asientos de inscripción de los ficheros de titularidad pública figurará, en todo caso, la información contenida en la disposición general de

creación o modificación del fichero, de conformidad con lo previsto en el artículo 18.2 de la Ley Orgánica 5/1992, de 29 de octubre.

3. En los asientos de inscripción de los ficheros de titularidad privada figurarán, en todo caso, la información contenida en la notificación del fichero a excepción de las medidas de seguridad, así como los cambios de finalidad del fichero, de responsable y de ubicación del fichero.

4. En los asientos de inscripción de cualesquiera ficheros de datos de carácter personal figurarán los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación y cancelación.

Artículo 25. *Actos y documentos inscribibles.*

Se inscribiran en el Registro General de Protección de Datos los siguientes actos y documentos:

a) Las autorizaciones de transferencia de datos personales a otros países, en los casos en que, a tenor de lo dispuesto en el artículo 32 de la Ley Orgánica 5/1992, de 29 de octubre, sea preceptiva para la transferencia la autorización previa del Director.

b) Los códigos tipo elaborados al amparo de lo previsto en el artículo 31 de la Ley Orgánica 5/1992.

Artículo 26. *Inscripción y certificaciones.*

1. Corresponde al Registro General de Protección de Datos instruir los expedientes de inscripción de los ficheros automatizados de titularidad privada y pública.

2. Corresponde asimismo al Registro General de Protección de Datos:

a) Instruir los expedientes de modificación y cancelación del contenido de los asientos.

b) Instruir los expedientes de autorización de las transferencias internacionales de datos.

c) Rectificar de oficio los errores materiales de los asientos.

d) Expedir certificaciones de los asientos.

e) Publicar una relación anual de los ficheros notificados e inscritos.

Sección 5.a

La Inspección de Datos

Artículo 27. *La Inspección de Datos.*

1. La Inspección de Datos es el órgano de la Agencia de Protección de Datos al cual competen las funciones inherentes al ejercicio de la potestad de inspección que el artículo 39 de la Ley Orgánica 5/1992, de 29 de octubre, atribuye a la Agencia.

2. Los funcionarios que ejerzan funciones inspectoras tendrán la consideración de autoridad pública en el desempeño de sus funciones, y estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 28. *Funciones inspectoras.*

1. Compete, en particular, a la Inspección de Datos efectuar inspecciones, periódicas o circunstanciales, de oficio o a instancia de los afectados, de cualesquiera ficheros, de titularidad pública o privada, en los locales en los que se hallen los ficheros y los equipos informáticos correspondientes, y a tal efecto podrá:

a) Examinar los soportes de información que contengan los datos personales.

b) Examinar los equipos físicos.

c) Requerir el pase de programas y examinar la documentación pertinente al objeto de determinar, en caso necesario, los algoritmos de los procesos de que los datos sean objeto.

d) Examinar los sistemas de transmisión y acceso a los datos.

e) Realizar auditorías de los sistemas informáticos con miras a determinar su conformidad con las disposiciones de la Ley Orgánica 5/1992.

f) Requerir la exhibición de cualesquiera otros documentos pertinentes.

g) Requerir el envío de toda información precisa para el ejercicio de las funciones inspectoras.

2. El responsable del fichero estará obligado a permitir el acceso a los locales en los que se hallen los ficheros y los equipos informáticos previa exhibición por el funcionario actuante de la autorización expedida por el Director de la Agencia. Cuando dichos locales tengan la consideración legal de domicilio, la labor inspectora deberá ajustarse además a las reglas que garantizan su inviolabilidad.

Artículo 29. *Funciones instructoras.*

Compete a la Inspección de Datos el ejercicio de los actos de instrucción relativos a los expedientes sancionadores a los que se refiere el artículo 12.2.h) del presente Estatuto.

Sección 6.8

La Secretaría General

Artículo 30. *Funciones de apoyo y ejecución.*

Corresponde a la Secretaria General:

a) Elaborar los informes y propuestas que le solicite el Director.

b) Notificar las resoluciones del Director.

c) Ejercer la Secretaria del Consejo Consultivo.

d) Gestionar los medios personales y materiales adscritos a la Agencia.

e) Atender a la gestión económico-administrativa del presupuesto de la Agencia.

f) Llevar el inventario de bienes y derechos que se integren en el patrimonio de la Agencia.

g) Gestionar los asuntos de carácter general no atribuidos a otros órganos de la Agencia.

Artículo 31. *Otras funciones.*

Corresponde asimismo a la Secretaria General:

a) Formar y actualizar un fondo de documentación sobre legislación, jurisprudencia y doctrina en materia de protección de datos personales y cualesquiera materias conexas.

b) Editar los repertorios oficiales de ficheros inscritos en el Registro General de Protección de Datos, las Memorias anuales de la Agencia y cualesquiera publicaciones de la Agencia.

c) Organizar conferencias, seminarios y cualesquiera actividades de cooperación internacional e interregional sobre protección de datos.

d) Facilitar la información a que se refiere el artículo 4.1 del presente Estatuto.

CAPITULO IV

Régimen económico, patrimonial y de personal

Sección 1.

Régimen económico

Artículo 32. *Recursos económicos.*

Los recursos económicos de la Agencia de Protección de Datos comprenderán:

a) Las asignaciones que anualmente se establezcan con cargo a los Presupuestos Generales del Estado.

b) Las subvenciones y aportaciones que se concedan a su favor, procedentes de fondos específicos de la Comunidad Económica Europea.

c) Los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades.

d) Las rentas y productos de los bienes, derechos y valores integrantes de su patrimonio.

e) El producto de la enajenación de sus activos.

f) Cualesquiera otros que legalmente puedan serle atribuidos.

Artículo 33. *Contabilidad y control.*

1. La Agencia de Protección de Datos ajustará su contabilidad al Plan General de Contabilidad Pública y a las demás disposiciones que sean de aplicación, sin perjuicio de la obligación de rendir cuentas al Tribunal de Cuentas por conducto de la Intervención General de la Administración del Estado, en los términos previstos en la Ley General Presupuestaria.

2. El ejercicio anual se computará por años naturales, comenzando el día 1 del mes de enero de cada año.

3. El control de las actividades económicas y financieras de la Agencia se ejercerá de conformidad con lo establecido en el artículo 17.1 de la Ley General Presupuestaria, con carácter permanente.

Artículo 34. *Presupuestos.*

1. La Agencia de Protección de Datos elaborará anualmente un anteproyecto de presupuesto, con la estructura que señale el Ministerio de Economía y Hacienda, y lo remitirá a éste para su ulterior elevación al Gobierno a fin de que sea integrado con la debida independencia en los Presupuestos Generales del Estado.

2. Las modificaciones del presupuesto de la Agencia serán autorizadas por el Director cuando se trate de modificaciones internas que no incrementen la cuantía del mismo y sean consecuencia de las necesidades surgidas durante el ejercicio.

3. Los suplementos de crédito o créditos extraordinarios de la Agencia serán autorizados por el Ministro de Economia Hacienda cuando no excedan del 5 por 100 de su presupuesto de gastos y por el Gobierno en los demás casos.

Sección 2.a

Régimen patrimonial

Artículo 35. *Patrimonio.*

1. La Agencia de Protección de Datos tendrá un patrimonio propio, distinto del Estado, formado por los bienes, derechos y valores que adquiera a título oneroso o le sean cedidos o donados por cualquier persona o entidad.

2. Los bienes que el Estado adscriba a la Agencia quedarán afectados a su servicio y conservarán la calificación jurídica originaria, debiendo ser utilizados eclusívamente para los fines que determinaron la adscrición.

Artículo 36. *Adquisiciones y contratación.*

1. La Agencia de Protección de Datos se regirá, en lo referente a las adquisiciones y enajenaciones de bienes, por las disposiciones del derecho privado.

2. Los bienes que adquiera la Agencia se integrarán en su patrimonio.

3. Los contratos que celebre la Agencia se regirán por las disposiciones del derecho privado, sin perjuicio de que la adjudicación de los contratos sea acordada previa publicidad y promoción de concurrencia.

Sección 3.a

Régimen del personal

Artículo 37. *Relación de puestos de trabajo.*

1. La Agencia de Protección de Datos propondrá a los órganos competentes, a través del Ministerio de Justicia, la relación de puestos de trabajo de la misma.

2. La relación de puestos de trabajo comprenderá:

a) Los puestos de trabajo a desempeñar por personal funcionario. Los titulares de los órganos a que se refiere el artículo 11.3 tendrán rango de Subdirector general.

b) Los puestos de trabajo a desempeñar por personal laboral, con expresión de los factores que, en función de las tareas integrantes de cada puesto de trabajo, determinen la imposibilidad de su desempeño por personal funcionario.

3. Las descripciones de los puestos de trabajo indicarán expresamente la obligación que, a tenor de lo previsto en los artículos 10 y 39 de la Ley Orgánica 5/1992, de 29 de octubre, corresponde al personal en lo relativo a la observancia de secreto sobre los datos personales, que los titulares de cada puesto conozcan en el desempeño de sus tareas.

Artículo 38. *Retribuciones.*

Las retribuciones del personal funcionario y laboral de la Agencia se ajustarán a lo dispuesto en las leyes anuales de presupuestos.

Artículo 39. *Provisión de puestos de trabajo.*

1. La Agencia de Protección de Datos proveerá los puestos de trabajo adscritos al personal funcionario ajustándose a la legislación de la Función Pública.

2. Los puestos de trabajo adscritos al personal laboral se proveerán mediante convocatoria pública y de acuerdo con los principios de igualdad, mérito y capacidad.

Disposiciones adicionales.

1. *El plazo para efectuar las propuestas de nombramiento.* En el plazo de un mes a contar de la entrada en vigor del presente Estatuto, las instituciones, órganos, corporaciones y organizaciones a que se refiere el artículo 19 del mismo, comunicarán los nombres de las personas que deban proponer para su nombramiento como miembros del Consejo Consultivo.

2. *Nombramiento de los miembros del Consejo Consultivo.* Transcurrido el plazo establecido en la disposición adicional primera, el Gobierno nombrará sin más trámite a los miembros del Consejo Consultivo que hubieran sido propuestos y designará de entre ellos al Director de la Agencia.

3. *Ficheros excluidos.*

a) En los términos y con los límites establecidos en los artículos 21.3 y 40 de la Ley Orgánica 5/1992 de 29 de octubre, quedan excluidos del ámbito de

aplicación del presente Estatuto los ficheros automatizados de Datos de Carácter Personal creados o gestionados por las Comunidades Autómomas.

b) Así mismo quedan excluidos del ámbito de aplicación del presente Estatuto los ficheros a los que se refiere el artículo 2, apartados 2 y 3, de la Ley Orgánica 5/1992 de 29 de octubre, salvo lo establecido en este último apartado para los ficheros que sirvan a fines exclusívamente estadísticos.

ANEXO IV

Ley 78-17 del 6 de enero de 1978
"LEY DE INFORMATICA, FICHEROS Y LIBERTADES" (Francia)

BERNARDO ALVAREZ ROJAS
Diploma de especialización en Derecho e informática de la Universidad de Montpellier
AUDILIO GONZALES AGUILAR
Doctor en Derecho e informática jurídica y miembro del grupo de investigación de la Universidad de Montpellier.

Presentamos a los lectores de habla española el texto de la ley 78-17 del 6 de enero de 1978 **"LEY DE INFORMATICA, FICHEROS Y LIBERTADES"** que constituye una referencia en la materia en toda Europa. Hemos considerado que dada la importancia que tiene en España con la existencia de un texto legal de la Ley Orgánica de tratamiento automatizado de los datos de carácter personal (LORTAD).

Hemos igualmente traducido los artículos del Código Penal francés que han modificado las sanciones (y por lo tanto constituyen un delito en derecho francés: artículos 226-16 al 226-24 del Código Penal -Libro II, Sección 5: Crímenes Y Delitos Contra Las Personas (Ley N° 92-1336 del 16 de Diciembre de 1992) por el tratamiento, utilización ilegal de datos de carácter personal.

Ley de Informática, Ficheros y Libertades.

Aprobada por la Asamblea Nacional y el Senado, el Presidente de la República promulga la siguiente ley:

CAPITULO I

Principios y Definiciones

Artículo 1.

La Informática estará al servicio de los ciudadanos. Su desarrollo se encuadrará en el marco de la cooperación internacional. No deberá atentar contra la identidad humana, los derechos humanos, la vida privada ni las libertades individuales o públicas.

Artículo 2.

Ningún fallo de los Tribunales de Justicia, que implique la apreciación de comportamientos humanos podrá tener por fundamento un tratamiento automático de información que pretenda dar una definición del perfil o la personalidad del interesado.

Ninguna decisión administrativa o privada que implique la apreciación de un comportamiento humano puede tener por único fundamento un tratamiento automático de información que pretenda dar una definición del perfil o la personalidad del interesado.

Artículo 3.

Todas las personas tienen el derecho de conocer y discutir las informaciones y razonamientos utilizados en los tratamientos automáticos cuyos resultados les sean adversos.

Artículo 4.

Se entienden como nominativas en el sentido de la presente ley las informaciones que permitan bajo cualquier forma, directa o indirectamente, la identificación de personas físicas, tanto si el tratamiento es efectuado por personas físicas o por personas morales.

Artículo 5.

Se entiende como tratamiento automático de informaciones nominativas en el sentido de la presente ley cualquier conjunto de operaciones realizadas por medios automáticos relativas a la recogida, registro, elaboración, modificación, conservación y destrucción de informaciones nominativas, así como cualquier conjunto de operaciones de la misma naturaleza que se refieran a la explotación de ficheros a bases de datos, y particularmente las interconexiones, consultas o comunicación de informaciones nominativas.

CAPITULO II

Comisión Nacional de Informática y Libertades

Artículo 6.

Se crea una Comisión Nacional de Informática y Libertades. Esta Comisión se encargará de velar por el respeto a las disposiciones de la presente ley, particularmente informando a las personas afectadas de sus derechos y obligaciones, y controlando las aplicaciones de la informática a los tratamientos de informaciones nominativas. A tal efecto, la Comisión dispondrá de poderes en los casos previstos por la presente ley.

Artículo 7.

Los fondos necesarios para el cumplimiento de las misiones de la Comisión serán inscritos en los presupuestos del Ministerio de Justicia. Las disposiciones de la ley de 10 de Agosto de 1922 relativas al control financiero no son aplicables a su gestión. La Comisión presentará sus cuentas al control del Tribunal de Cuentas.

En cualquier caso, los gastos precisos para el cumplimiento de las formalidades referidas en los artículos 15, 16, 17 y 24 de la presente ley podrán ser reintegrados.

Artículo 8.

La Comisión Nacional de Informática y Libertades es una autoridad administrativa independiente.

Se compondrá de diecisiete miembros nominados por cinco años o por el tiempo de ocupación del cargo que les asigne en calidad de miembro:

- Dos diputados y dos senadores elegidos respectivamente por la Asamblea Nacional y el Senado.

- Dos miembros del Consejo Económico y Social elegidos por esta Asamblea.

— Dos miembros o antiguos miembros del Consejo de Estado, uno de ellos con categoría al menos igual a la de Consejero, elegidos por la Asamblea General del Consejo de Estado.

— Dos miembros o antiguos miembros del Tribunal de Casación, uno de ellos con categoría al menos igual a la de Consejero, elegidos por la Asamblea General de este Tribunal.

— Dos miembros o antiguos miembros del Tribunal de Cuentas, uno de ellos con categoría al menos igual a la de Consejero, elegidos por la Asamblea General de este Tribunal.

— Dos personas reputadas por su conocimiento de las aplicaciones de la informática, nombradas por decreto a propuesta, respectivamente, de los Presidentes de la Asamblea Nacional y del Senado.

— Tres personalidades nombradas, en razón de su autoridad y su competencia, por decreto en Consejo de Ministros.

La Comisión elegirá de entre sus miembros, por un mandato de cinco años, un Presidente y dos Vicepresidentes.

La Comisión establecerá su propio reglamento de régimen interior.

En caso de igualdad de votos, decidirá el del Presidente.

Si durante su mandato, el Presidente o algún miembro cesara en el ejercicio de su función, el mandato de su sucesor se limitará al período restante a cubrir.

La calidad de Miembro de la Comisión es incompatible:

— Con la de Miembro del Gobierno.

— Con el ejercicio de funciones o la posesión de intereses en empresas que se dediquen a la fabricación de material utilizado en informática o telecomunicaciones o a la prestación de servicios en dichos campos.

La Comisión decidirá en cada caso las incompatibilidades que puede imponer a sus miembros.

Salvo por decisión, las funciones de los miembros no pueden finalizar excepto por impedimento constatado por la Comisión en las condiciones que ésta defina.

Artículo 9.

El Primer Ministro designará un representante del Gobierno cerca de la Comisión.

Este podrá imponer nueva deliberación en los diez días siguientes al término de una segunda deliberación.

Artículo 10.

La Comisión dispondrá de servicios bajo la autoridad del Presidente o, por delegación, de un Vicepresidente.

La Comisión podrá delegar en su Presidente o, pór delegación, en un Vicepresidente, en ejercicio de sus atribuciones en lo que concierne a la aplicación de los artículos 16, 17 y 21 (4°, 5° y 6°).

Los Agentes de la Comisión Nacional serán nombrados por el Presidente o un Vicepresidente delegado.

Artículo 11.

La Comisión podrá pedir a los primeros Presidentes de Tribunales de Apelación o a los Presidentes de Tribunales Administrativos la delegación de uno de sus Magistrados, eventualmente asistido por expertos en la materia, para misiones de investigación y control bajo su dirección.

Artículo 12.

Los miembros y los agentes de la Comisión estarán obligados al secreto profesional en lo que concierne a los hechos, actuaciones o informaciones de

los que hayan tenido conocimiento en razón de sus funciones, en las condiciones previstas en el artículo 75 del Código Penal, y en lo que sea necesario para la emisión del informe anual previsto en esta ley, según el artículo 378 del Código Penal.

Artículo 13.

En el ejercicio de sus atribuciones, los miembros de la Comisión Nacional de Informática y Libertades y los miembros de las Delegaciones Regionales no estarán bajo el mando de ninguna autoridad. Los informáticos llamados a declarar por la Comisión quedarán liberados para ello de sus obligaciones de discreción.

CAPITULO III

Formalidades Previas a la puesta en marcha de Tratamientos Automáticos

Artículo 14.

La Comisión Nacional de Informática y Libertades velará para que los tratamientos automatizados, públicos o privados, de informaciones nominativas, sean efectuados de acuerdo a las disposiciones de la presente ley.

Artículo 15.

Excepto en los casos en que deban ser autorizados por ley, los tratamientos automáticos de informaciones nominativas efectuados por cuenta del Estado, de instituciones públicas, de colectividades territoriales o de personas morales de derecho privado que presten servicios públicos serán autorizados por ley o por un acta reglamentaria emitida tras recibir autorización de la Comisión Nacional de Informática y Libertades.

Si no se recibiera autorización de la Comisión, podrá ser puesto en marcha sólo por decreto autorizado por el Consejo de Estado, o bien, en caso de las colectividades territoriales, en virtud de acuerdos de su órgano ejecutivo instalarlos por decreto tras la autorización del Consejo de Estado.

Si transcurrido un plazo de dos meses, renovable una sóla vez por decisión del Presidente, el informe de la Comisión no ha sido recibido, se supondrá favorable.

Artículo 16.

Los tratamientos automáticos de informaciones nominativas efectuados por otras personas de las que figuran en el artículo 15 deberán ser precedidas de una declaración enviada a la Comisión Nacional de Informática y Libertades.

Esta declaración implica la presunción de que el tratamiento satisface las exigencias de la Ley.

El peticionario podrá poner en marcha el tratamiento en cuanto tenga en su poder el aviso de recepción, que será librado sin demora. Lo anterior no le eximirá de sus responsabilidades.

Artículo 17.

Para los tratamientos más usuales, de carácter público o privado, de los que no pueda sospecharse en principio que atenten contra la vida privada o las libertades, la Comisión dictará y publicará normas simplificadas de acuerdo a las características citadas en el artículo 19.

Este tipo de tratamientos sólo precisarán de la entrega a la Comisión de una declaración simplificada, según una de dichas normas. Excepto por decisión concreta de la Comisión, el aviso de recepción de la declaración se librará sin demora. El peticionario podrá poner en marcha el tratamiento en cuanto tenga en su poder el aviso citado. Lo anterior no le eximirá de sus responsabilidades.

Artículo 18.

La utilización del fichero nacional de identificación de personas físicas con objeto de efectuar tratamientos nominativos deberá autorizarse por decreto en Consejo de Estado tras recibir autoriza ción de la Comisión.

Artículo 19.

Las declaraciones o peticiones de autorización mencionadas deberán precisar los siguientes puntos:

— Persona que presenta la petición y que puede ordenar la puesta en marcha del tratamiento o su representante en Francia si aquélla residiese en el extranjero.

— Características, finalidad y eventualmente, denominación del tratamiento.

- Servicio o servicios encargados de la puesta en marcha.

- Servicio que facilitará el acceso especificado en el Capítulo V de esta ley, las medidas tomadas para facilitar el ejercicio de este derecho.

— Personas que por razón de su función o necesidades de su servicio tendrán acceso a las informaciones registradas.

— Informaciones nominativas objeto del tratamiento, su origen y duración de su conservación, así como sus destinatarios autorizados.

— Interconexiones a cualquier forma de relación de estas informaciones, así como su cesión a terceros.

— Medidas previstas para garantizar la seguridad de los tratamientos e informaciones, y la garantía de los secretos protegidos por la ley.

— Si el tratamiento se destina a transmitir informaciones nominativas entre el territorio francés y el extranjero bajo cualquier forma, incluyendo los casos en que se trate de operaciones a realizar en territorio francés a partir de otras operaciones efectuadas fuera de él.

Cualquier modificación de las condiciones enumeradas o supresión de tratamientos deberá ser comunicada a la Comisión.

En las peticiones de autorización de tratamientos automáticos que afecten a la seguridad del Estado, la defensa a la seguridad pública pueden no incluir algunas de las características mencionadas.

Artículo 20.

El acta reglamentaria prevista en los casos definidos en el artículo 15 precisará en particular:

— Denominación y fines del tratamiento.

— Servicio que facilitará el acceso especificado en el Capítulo V.

- Tipo de informaciones nominativas registradas, así como sus destinatarios autorizados.

— Por decretos del Consejo de Estado puede determinarse la no publicación de las actas reglamentarias que se refieran a tratamientos que afecten la seguridad del Estado, la defensa o la seguridad pública.

Artículo 21.

Para el ejercicio de su función de control, la Comisión:

1° Tomará decisiones individuales o reglamentarias en los casos previstos por la presente ley.

2° Podrá encargar a uno o varios de sus miembros o agentes, asistidos si es preciso por expertos, la investigación y verificación "in situ" de cualquier tratamiento, pudiendo éstos exigir toda clase de explicaciones y documentos útiles para su misión.

3° Dictará en caso de necesidad reglamentos que garanticen la seguridad de los sistemas, pudiendo llegar en casos excepcionales a imponer medidas de seguridad que lleguen incluso a la destrucción de los soportes de información.

4° Podrá enviar avisos a las personas interesadas, y denunciará las infracciones de las que tenga conocimiento, de acuerdo al artículo 40 del código de procedimiento penal.

5° Velará para que las formas de ejercicio de los derechos de acceso y rectificación indicados en las actas y declaraciones previstas en los artículos 15/16 no dificulten el libre ejercicio de estos derechos.

6° Recibir las reclamaciones, peticiones y súplicas.

7° Se mantendrá informada de las actividades industriales y de servicios que concurren al desarrollo de la informática.

Los ministros, autoridades públicas, directivos de empresas públicas o privadas, responsables de todo tipo de asociación y más generalmente los poseedores o usuarios de ficheros nominativos no podrán oponerse a las acciones de la Comisión o de sus miembros por ningún motivo, y deberán por el contrario prestarles cuanta ayuda precisen para el ejercicio de su cargo.

Artículo 22.

La Comisión pondrá a disposición del público una lista con los tratamientos autorizados, precisando en cada caso:

— La ley o el acta reglamentaria que autorizan su creación, o bien la fecha de la declaración.

— Su denominación y finalidad.

— El servicio que facilita el derecho de acceso previsto en el Capítulo V de esta ley.

— Los tipos de informaciones nominativas registradas, así como sus destinatarios autorizados.

Se mantendrán a disposición del público, en condiciones fijadas por decreto, las decisiones, autorizaciones y recomendaciones de la Comisión cuyo conocimiento sea útil para la aplicación o interpretación de la presente ley.

Artículo 23.

La Comisión presentará cada año al Presidente de la República y al Parlamento un informe dando cuenta de la ejecución de su misión. Este informe será publicado.

El citado informe describirá en particular los procedimientos y métodos de trabajo seguidos por la Comisión, y contendrá como anexos todo tipo de datos sobre la organización de la Comisión y sus servicios, destinados a facilitar la relación del público con ellos.

Artículo 24.

A propuesta o autorización de la Comisión, la transmisión de informaciones nominativas entre el territorio francés y el extranjero bajo cualquier forma, que sean objeto de tratamientos automáticos citados en el artículo 16 podrá estar sujeta a autorización previa o reglamentaria según modalidades fijadas en Consejo de Estado, a fin de asegurar el respeto de los principios estipulados por la presente ley.

CAPITULO IV

Captura, Registro y Conservación de Informaciones Nominativas

Artículo 25.

Se prohibe la recogida de datos por cualquier medio fraudulento, ilegal o ilícito.

Artículo 26.

Las personas físicas tienen el derecho de oponerse por motivos justificados a que las informaciones nominativas que les conciernan sean objeto de tratamiento.

En derecho no se aplicará a los tratamientos designados por el acta reglamentaria prevista por el artículo 15.

Artículo 27.

Las personas a las que se refieren informaciones nominativas deben ser informadas:

- del carácter obligatorio o voluntario de sus respuestas,

— de las implicaciones de su negativa a informar,

- de las personas físicas o morales destinatarias de las informaciones,

- de la existencia de los derechos de acceso y rectificación.

Cuando las informaciones sean recogidas por medio de cuestionarios éstos deberán incluir dichas notificaciones.

Esta disposición no se aplicará en la recogida de información dedicada a la constatación de infracciones.

Artículo 28.

Salvo disposiciones legales en contra, las informaciones nominativas no deberán conservarse como nominativas por más tiempo del especificado en la

petición de autorización o en la declaración, excepto si su conservación es autorizada por la Comisión.

Artículo 29.

Cualquier persona que ordene o ejecute el tratamiento de informaciones nominativas se obliga a tomar, de acuerdo con las personas afectadas, todo tipo de precauciones dirigidas a garantizar la seguridad de dichas informaciones, y en particular impedir que sean deformadas, dañadas o comunicadas a terceros no autorizados.

Artículo 30.

Salvo disposiciones legales en contra pueden proceder al tratamiento automático de informaciones nominativas dirigidas al control de infracciones, condenas o medidas de seguridad las jurisdicciones y autoridades públicas en que ello entre en el marco de sus atribuciones legales, así como, por autorización de la Comisión, las personas morales encargadas de servicios públicos.

Hasta la creación del fichero previsto por la ley 70-539 de 24 de Junio de 1970, las empresas de seguros son autorizadas, bajo control de la Comisión, a tratar por si mismas las informaciones mencionadas en el artículo 5 de dicha ley, concernientes a las personas mencionadas en el último inciso de dicho artículo.

Artículo 31.

Se prohibe, salvo autorización expresa del interesado, grabar, conservar en soportes informáticos datos nominativos que directa o indirectamente se refieren al origen racial, las creencias políticas, filosóficas o religiosas o la afiliación sindical de las personas.

Sin embargo, las iglesias y las asociaciones de carácter religioso, filosófico, político o sindical podrán mantener registros automatizados de sus miembros o colaboradores, sin que pueda ejercerse a este objeto ningún control sobre ellas.

También podrá desestimarse la prohibición mencionada, por motivos de interés público, a propuesta o por autorización de la Comisión por decreto en Consejo de Estado.

Artículo 32.

Los ficheros electorales se pondrán a disposición de los candidatos y de los partidos políticos en idénticas condiciones para todos ellos, bajo el control de las Comisiones de propaganda electoral.

Artículo 33.

Las disposiciones de los artículos 24, 30 y 31 no se aplicarán a las informaciones nominativas tratadas por los organismos de la prensa impresa o audiovisual, en el marco de las leyes que les afectan y en los casos en que su aplicación tuviera por efecto la limitación del ejercicio de la libertad de expresión.

CAPITULO V

Ejercicio del Derecho de Acceso

Artículo 34.

Todas las personas tienen el derecho, demostrando su identidad, de consultar a los organismos encargados de la ejecución de los tratamientos automatizados cuya lista es accesible al público por la aplicación del artículo 22 de la presente ley, con objeto de saber si estos tratamientos incluyen informaciones nominativas que les conciernan, así como de obtener comunicación de ellas si así fuera.

Artículo 35.

El titular del derecho de acceso podrá obtener comunicación de las informaciones que le conciernan. Esta comunicación deberá darse en formato fácilmente inteligible y correponder al contenido de lo registrado.

Se entregará una copia al titular del derecho de acceso que lo solicite, contra percepción de un abono global variable según la categoría del tratamiento, cuyo importe se fijará por decisión de la Comisión, homologada por el Ministerio de Economía.

En cualquier caso, la Comisión, a petición del responsable del fichero, podrá:

- fijar plazos de respuesta,

- autorizar que se desestimen las peticiones claramente abusivas por su número o su carácter repetitivo o sistemático.

Cuando exista temor fundado de encubrimiento o desaparición de las informaciones mencionadas en el primer párrafo del presente artículo, incluso con anterioridad al ejercicio de un recurso jurisdiccional, podrá pedirse al juez competente que se ordenen medidas de cualquier tipo a fin de evitar dichos encubrimientos o desapariciones.

Artículo 36.

El titular del derecho de acceso podrá exigir que las informaciones inexactas, incompletas, equívocas, obsoletas o cuya recogida, utilización, comunicación o conservación ha sido prohibida y que le conciernan sean rectificadas, completadas, clarificadas, actualizadas o borradas.

Cuando así lo pida el interesado, el servicio u organismo afectado emitirá sin cargo una copia de la grabación modificada.

En los casos en que exista reclamación, los gastos de la prueba serán por cuenta del servicio que facilita el derecho de acceso, excepto si se demuestra que las informaciones han sido facilitadas por el interesado o con su consentimiento.

Cuando el titular del derecho de acceso obtenga la modificación de las grabaciones, se le reintegrará el abono librado en virtud del artículo 35.

Artículo 37.

Los ficheros nominativos deberán ser completados o corregidos en cuanto el organismo que los posea tenga conocimiento de la inexactitud o del carácter incompleto de las informaciones nominativas contenidas en él.

Artículo 38.

Si una información ha sido transmitida a un tercero, deberá notificársele su rectificación o anulación, salvo dispensa de la Comisión.

Artículo 39.

Las reclamaciones sobre tratamientos que afecten a la seguridad del Estado, la defensa o la seguridad pública serán enviadas a la Comisión, que desig-

nará a uno de sus miembros, que pertenezca o haya pertenecido al Consejo de Estado, al Tribunal de Casación o al Tribunal de Cuentas, para que efectúe las investigaciones pertinentes y ordene la ejecución de las correspondientes modificaciones. El miembro designado al efecto podrá ser asistido por un agente de la Comisión.

Se notificará al reclamante que se han efectuado verificaciones al respecto.

Artículo 40.

Cuando el ejercicio del derecho de acceso se aplique sobre informaciones médicas, éstas deberan ser comunicadas al interesado por medio de un médico que él designe.

CAPITULO VI

Disposiciones Penales

Artículo 41.

Las infracciones a las disposiciones de la presente ley son consideradas por los artículos 226-16 al 226-24 del Código Penal (Ley n° 92-1336 del 16 de diciembre de 1992).

Código Penal -Libro II, Sección 5: Crímenes y Delitos contra las personas (Ley N° 92-1336 del 16 de Diciembre de 1992)

De los ficheros o tratamientos informáticos que violan los derechos de la persona (Artículos 42, 43 y 44)

Artículo 226-16.

La utilización de tratamientos automatizados de informaciones nominativas que no han respetado las formalidades que preceden esta utilización, tiene una pena de tres años de prisión y 300.000 F. de multa.

Artículo 226-17.

La utilización de tratamientos automatizados de informaciones nominativas sin tomar todas las precauciones útiles para preservar la seguridad de

dichas informaciones, y en particular para evitar que sean deformadas, deterioradas o comunicadas a terceros no autorizados, tiene una pena de cinco años de prisión y 2.000.000 F. de multa.

Artículo 226-18.

El recolectar los datos por un medio fraudulento, desleal o ilícito, o el utilizar un tratamiento de informaciones nominativas que conciernen una persona física a pesar de que ella se oponga. Cuando esta oposición es legítimamente fundada, está penalizado con cinco años de prisión y con 2.000.000 F. de multa.

Artículo 226-19.

El hecho, fuera de los casos previstos en la ley, de introducir o de conservar en memoria informatizada, sin el acuerdo expreso del interesado, datos nominativos que, directamente o indirectamente, revelen los orígenes raciales, o las opiniones políticas, filosóficas o religiosas, o las vinculaciones sindicales, o los hábitos de las personas, está penalizado con cinco años de prisión y con 2.000.000 F. de multa.

El hecho, fuera de los casos previstos en la ley, de introducir o de conservar en memoria informatizada las informaciones nominativas concernientes a las infracciones, las condenas o las medidas preventivas.

Artículo 226-20.

El hecho de, sin el acuerdo de la Comisión Nacional de la Informática y de las Libertades, conservar las informaciones bajo una forma nominativa, mas allá del tiempo establecido al momento de la solicitud ante la Comisión, o de la declaración previa al funcionamiento del tratamiento informatizado, está penalizado con tres años de prisión y con 300.000 F. de multa.

Artículo 226-21.

El hecho, para toda persona que posee informaciones nominativas al momento de su grabación, de su clasificación, de su transmisión o de cualquier otro tipo de tratamiento, de desviar estas informaciones de la finalidad fijada por ley o decreto que autoriza el tratamiento automatizado, o por las declaraciones previas al funcionamiento del tratamiento, está penalizado con cinco años de prisión y con 2.000.000 F. de multa.

Artículo 226-22.

El hecho, para toda persona que ha colectado, al momento de su grabación, de su clasificación, de su transmisión o de cualquier otro tipo de tratamiento, informaciones nominativas, cuya divulgación puede menoscabar la persona interesada, en la intimidad de su vida privada, de comunicar, sin la autorización del interesado, dichas informaciones a un tercero que no ha sido facultado para recibirlas, está penalizado con un año de prisión y con 100.000 F de multa.

La divulgación prevista en el inciso anterior, está penalizada con 50.000 F. de multa, cuando se realiza por imprudencia o negligencia.

En los casos contemplados en los dos incisos precedentes, sólo la demanda de la víctima, de su representante legal, o de sus derechohabientes, pone en marcha el proceso.

Artículo 226-23.

Las disposiciones de los artículos 226-17 al 226-19 se aplican a los ficheros manuales o mecanografiados, cuyo uso no implica exclusivamente el derecho a la vida privada.

Artículo 226-24.

Las personas morales pueden ser declaradas responsables penalmente, según las condiciones previstas por el artículo 121-2, de las infracciones definidas en los artículos 226-21 al 226-23, así como el primer inciso del artículo 226-22.

Las penas establecidas para las personas morales son:

1° La multa, según las diferentes modalidades previstas por el artículo 31-38;

2° Las penas mencionadas en los ordinales 2°, 3°, 4°, 5°, 7°, 8° y 9° del artículo 131-39.

La infracción mencionada en el ordinal 2° del artículo 131-39, versa sobre la actividad en el ejercicio de la cual se cometió.

CAPITULO VII

Disposiciones Diversas

Artículo 45.

Las disposiciones de los artículos 25, 27, 29, 30, 31, 32 y 33 relativas a la recogida, registro y conservación de informaciones nominativas serán aplicables a los ficheros no automatizados o mecanográficos, con excepción de aquellos cuyo uso se enmarca en el estricto ejercicio del derecho a la vida privada.

El primer párrafo del artículo 26 será aplicable a estos mismos ficheros, con excepción de los ficheros públicos establecidos por un acta reglamentaria.

Cualquier persona que justifique su identidad tendrá derecho a consultar a los servicios u organismos que posean dichos ficheros con objeto de saber si éstos contienen informaciones nominativas que le conciernan. El titular del derecho de acceso podrá obtener comunicación de estas informaciones podrá exigir asimismo la aplicación de los tres primeros párrafos del artículo 36 de la presente ley relativos al derecho de rectificación. También serán de aplicación los artículos 37, 38, 39 y 40. Por decreto del Consejo de Estado se fijarán las condiciones del ejercicio de los derechos de acceso y rectificación; este decreto podrá prever la percepción de abonos para la emisión de copias de las informaciones comunicadas.

El Gobierno podrá decidir por decreto del Consejo de Estado, a propuesta de la Comisión Nacional de Informática y Libertades, la aplicación total o parcial de las demás disposiciones de la presente ley a los ficheros no automatizados o mecanográficos que impliquen peligro en la protección de las libertades, por sí mismos o en base a su combinación con ficheros informáticos.

Artículo 46.

Las normas de aplicación de la presente ley serán fijadas por decretos en Consejo de Estado. Deberán dictarse en un plazo de seis meses a partir de su promulgación.

Estos decretos determinarán los plazos de entrada en vigor de las disposiciones de la presente ley. Estos plazos no podrán exceder de dos años a partir de la promulgación de dicha ley.

Artículo 47.

La presente ley es aplicable a Mayotte y a los territorios de ultramar.

Artículo 48.

A título transitorio, los tratamientos contemplados en el artículo 15 ya en marcha sólo estarán sujetos a una declaración presentada a la Comisión Nacional de Informática y Libertades en las condiciones previstas por los artículos 16 y 17.

A la expiración de dicho plazo, contado a partir de la promulgación de la presente ley, todos los tratamientos regidos por el artículo 15 deberán ser conformes a lo estipulado en este artículo.

La presente ley tendrá el rango de ley del Estado.

París, 6 de Enero de 1978

VALERY GISCARD D'ESTAING
Por el Presidente de la República.

El Primer Ministro
RAYMOND BARRE

El Ministro del Interior
CHRISTIAN BONNET

El Ministro de Justicia
ALAIN PEYRE FITTE

El Ministro de Defensa
YVON BOURGES

El Ministro de Economía y Finanzas
ROBERT BOULIN

El Ministro de Equipamiento y Conservación del Territorio
FERNAND ICART

El Ministro de Educación
RENE HABY

El Ministro de Trabajo
CHRISTIAN BEULLAC

El Ministro de Industria Comercio y Artesanado
RENE MONORY

El Ministro de Sanidad y Seguridad Social
SIMONE VEIL

Normas de Presentación de Trabajos de la Revista Informática y Derecho

1º Todos los trabajos deberán presentarse escritos a ordenador en cualquiera de los procesamientos de textos siguientes:

Sistemas PC/PS:

- Formato ASCII
- Microsoft WORD para DOS
- Wordperfert para DOS
- Lotus Amipro para WINDOWS
- Write WINDOWS
- Word para WINDOWS

2º Estos archivos de textos deberán ser entregados en disketes de 3,5 " y en la etiqueta del mismo se deberá especificar el nombre del archivo y el procesamiento de textos utilizado para su elaboración.

3º Es imprescindible adjuntar con los disketes dos copias en soporte papel.

4º El título de los trabajos deberá ser muy claro y preciso, figurando en la cabecera en letras mayúsculas. Debajo irá el nombre del autor, también en mayúsculas, y por último el nombre del Departamento, Universidad, Centro o institución a donde pertenezca el autor/es y su posición en el mismo, o titulación académica.

5º A continuación de la cabecera deberá ir un resumen de 75 a 100 palabras, especificando el objeto del trabajo, las fuentes documentales, la elaboración de datos y experiencias expuestas, y las conclusiones del mismo. Estará redactado en español y aconsejable en inglés y francés.

6º Las notas se enumerarán correlativamente, debiendo incluirse como pies de páginas, mecanografiadas a un sólo espacio; reduciéndose las referencias a lo mínimamente indispensable, evitándose los comentarios extensos sobre las citas mencionadas.

7º La extensión máxima de los artículos, salvo aprobación por la revista, no podrán exceder de 30 folios y deberán realizarse en formato A-4 por una sola cara y con un interlineado doble, dejando márgenes laterales de 3 cm. y los superiores e inferiores de 4 cm. aproximadamente.

8º Las ponencias deberán ser entregadas o remitidas a la Secretaría del Centro Regional de la U.N.E.D. en Extremadura, sito en calle Moreno de Vargas, Nº 10 - 06800 Mérida (España). Tfnos: 34-24-315050/11 Fax: 34-24-302556

9º Para mayor información dirijirse a la dirección anterior o a los Tfnos: 34-24-315050/11 y Fax: 34-24-302556.

COLECCION INFORMATICA Y DERECHO

REVISTA Nº 1

- CONTRATOS INFORMATICOS
- DOCUMENTO ELECTRONICO
- DERECHO A LA INTIMIDAD
- INTELIGENCIA ARTIFICIAL
- TECNOLOGIAS DE LA INFORMACION
- TERRORISMO POR COMPUTADORA
- BASES DE DATOS
- HABEAS DATAS

REVISTA Nº 2 EL DERECHO DE LA PRUEBA Y LA INFORMATICA

REVISTA Nº 3 RESUMEN DE LAS COMUNICACIONES DE III CONGRESO IBEROAMERICANO DE INFORMATICA Y DERECHO

REVISTA Nº 4 ACTAS DEL III CONGRESO IBEROAMERICANO DE INFORMATICA Y DERECHO (VOLUMEN I)

- PROTECCION DE DATOS
- CONTRATACION INFORMATICA
- PROTECCION DE SOFTWARE
- DELITOS INFORMATICOS
- REGULACION JURIDICA DE LA INFORMATICA LAS TELECOMUNICACIONES
- IMPACTO DE LA INFORMATICA EN EL DERECHO

REVISTA Nº 5 ACTAS DEL III CONGRESO IBEROAMERICANO DE INFORMATICA Y DERECHO (VOLUMEN II)

- BASES DE DATOS JURIDICOS
- HIPERTEXTO E INFORMATICA LEGISLATIVA
- INFORMATICA DECISIONAL Y SISTEMAS EXPERTOS
- INFORMATICA JUDICIAL
- INFORMATICA JURIDICA Y REGISTRAL
- PROCESO INFORMATIZADO Y DERECHO DE LA PRUEBA
- PANORAMA IBEROAMERICANO DE LA INFORMATICA Y EL DERECHO