

# 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 <sup>1</sup> 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.

madras 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 <sup>2</sup> sino que emplea el restrictivo “limitará” <sup>3</sup>. 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 prohíbe, 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<sup>4</sup>, 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”<sup>5</sup>, 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<sup>6</sup> 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 menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.*

■ 5 “Si 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<sup>7</sup> 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<sup>8</sup> como el derecho de ser dejado a solas. Pero en España se utiliza el término "intimidad", del que ya nos ocupamos en otro lugar<sup>9</sup>. Los redactores de la Exposición de Motivos pretenden realizar una diferenciación entre "privacidad", considerándola como el conjunto de elementos que, separadamente no son trascendentes, 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<sup>10</sup>, 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 Alfíl. 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 sólo 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) <sup>11</sup> 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. Únicamente en el caso de que se piense que los datos de un fichero pueden ser sensibles sólo 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<sup>12</sup> 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 INFORMÁTICA 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 <sup>13</sup>, 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 <sup>14</sup> 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 <sup>15</sup> 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<sup>16</sup> 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 gratuita"*.

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<sup>17</sup>, 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 rectificadas 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<sup>18</sup>, 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 rectificadas y cancelados en su caso.

3.- Si los datos rectificadas 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<sup>19</sup> que nace ya bajo la duda de su inconstitucionalidad.

Así, López Garrido<sup>20</sup> 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 acción 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 característica 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<sup>21</sup>.

### **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 <sup>22</sup> 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 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 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 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.

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<sup>23</sup> 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 sólo 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 <sup>24</sup>.

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 2º.

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 o 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 <sup>25</sup> 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 Higuera, Luis Navarro Gil y Ramón Villanueva Etcheverría.